digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Janina Rochon

Questionable Control.

The Legal Classification of Personal Information Management Systems under the GDPR and beyond.

Band 33

Janina Rochon

Questionable Control

Controllership and Liability in Personal Information Management Systems

digital | recht
Schriften zum Immaterialgüter-, IT-, Medien-, Daten- und Wettbewerbsrecht

Herausgegeben von Prof. Dr. Maximilian Becker, Prof. Dr. Katharina de la Durantaye, Prof. Dr. Franz Hofmann, Prof. Dr. Ruth Janal, Prof. Dr. Anne Lauber-Rönsberg, Prof. Dr. Benjamin Raue, Prof. Dr. Herbert Zech

Band 33

Janina Rochon, geboren 1991, Zur Person: Studium der Rechtswissenschaften an der Europa Universität Viadrina und der Adam Mickiewicz Universität in Posen; seit 2017 tätig im Bereich Datenschutz, sowohl im privaten, als auch öffentlichen Bereich; Certified Information Privacy Professional und Certified Information Privacy Manager, seit 2020 Arbeit im Leitungsbüro des Bundesinstitutes für Risikobewertung in verschiedenen Funktionen.

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.
Dieses Buch steht gleichzeitig als elektronische Version über die Webseite der Schriftenreihe: http://digitalrecht-z.uni-trier.de/ zur Verfügung.

Umschlagsgestaltung von Monika Molin

ISBN: 9783565425211
URN: urn:nbn:de:hbz:385-2510091434547.912400577854
DOI: https://doi.org/10.25353/ubtr-7eec-2967-4ea6

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).
Anschrift der Herausgeber: Universitätsring 15, 54296 Trier.

UNIVERSITÄT TRIER

IRDT Institut für Recht und Digitalisierung Trier

Vorwort

The present dissertation was written as part of the doctoral procedure at the Chair for Law and Ethics of the Digital Society at the European New School of Digital Studies (ENS) at European University Viadrina Frankfurt (Oder) under the supervision of Prof. Dr. Philipp Hacker. It deals with the question of which role under the GDPR should be assigned to Personal Information Management Systems and proposes solutions aimed at greater consistency and legal clarity.

While I am both proud and grateful to have completed this work, it would not have been possible without the extraordinary support of many people. I sincerely hope they are aware of how important their contributions have been, and I would like to take this opportunity to express my heartfelt thanks.

First and foremost, I would like to thank my supervisor, Prof. Dr. Philipp Hacker. His insight and expertise have been invaluable to the development of this thesis. It should also be mentioned that, while I was working at the Chair for Law and Ethics of the Digital Society, Prof. Hacker always made sure not to give me too many assignments so that I had enough time to work on this thesis. Without his consideration, which is in no way a given in academia, I would never have been able to complete this work.

Secondly, I wish to thank my second examiner, Prof. Dr. Jan-Erik Schirmer, for the careful and prompt review of the dissertation and the valuable suggestions he has made.

Furthermore, I would also like to thank my colleagues at the Federal Institute for Risk Assessment (Bundesinstitut für Risikobewertung), who took over my tasks while I was taking time off to finish the thesis.

Knowing that they had everything under control enabled me to fully focus on the thesis while I was away from work. This applies to all of my colleagues in the executive office. Special thanks go to Heike Strecker and Dr. Magnus Jäger, who likely suffered the most from my frequent “PhD vacations”.
Moreover, there are two women who have both inspired and supported me throughout this journey: Dr. Marit Hansen, who was kind enough to take the time to mentor me for one year, and Prof. Dr. Tanja Schwerdtle, whom I had the honor of working for between 2020 and 2024. They have both pushed and encouraged me at the same time, and their incredible strength, brilliance, work ethic, and leadership skills have given me something to aspire to.
I am also profoundly grateful to my family for their support, patience, and belief in me throughout this journey. My parents, Agnieszka and Sebastian Rochon, have stood behind me, quite literally since I was born, and always made sure that I had the strength and confidence to pursue my dreams. I am likewise grateful to Dr. Silvia Pena, who has always found kind and supportive words for me, giving me strength.
Then, of course, my partner, the wonderful and magnificent Dr. Rodrigo Kaufmann, who has been both my rock and lifeline over these past years. He endured every bad mood and unwaveringly supported me through all of those days filled with frustration, tiredness, self-doubt, and impatience. Moreover, he gave me the gift of time, taking over not just mundane domestic duties, but, most importantly, caring for our daughter while I was away at the library. This thesis would never have been completed without his immense support.
Finally, since my daughter has already been mentioned, her contribution to this work should also not be underestimated. While doctoral students are notoriously known for rewriting, rereviewing, and generally being stuck in a loop of never-ending corrections and perfectionism, she very effectively protected me from this sickness. Her irresistibly sweet smile, combined with persistent questions such as “Can we play?” and “When will you come back?”, ensured that “good enough” remained the standard and that this work could reach its glorious conclusion. Thank you!

Berlin, April, 2026
Janina Rochon

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AcP	Archiv für die civilistische Praxis
AI	Aritifical Inteligence
AIA	AI Act
AfP	Archiv für Presserecht, ab 1994: Zeitschrift für Medien- und Kommunikationsrecht
arg.	argumentum
Art.	Artikel
Art. 29 WP	Art. 29 Working Party
Aufl.	Auflage
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs
BReg	Bundesregierung
BT-Drucks.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
CJEU	Court of Justice of the European Union
CLSR	Computer Law & Security Review
COM	European Commission
CR	Computer und Recht
CR Int.	Computer und Recht International

DesignG	Gesetz über den rechtlichen Schutz von Design
DFG	Deutsche Forschungsgemeinschaft
DGA	Data Governance Act
Diss.	Dissertation
DMA	Digital Markets Act
DRMS	Digital Rights Management System
DSGVO	Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit
EDPL	European Data Protection Law Review
ELI	European Law Institute
E.R.P.L.	European Review of Private Law
etc.	et cetera
EU	European Union
EuCML	Journal of European Consumer and Market Law
f., ff.	following
Fn.	Footnote
FS	Festschrift
FTC	Federal Trade Commission
FRA	European Union Agency for Fundamental Rights
G-BA	Gemeinsamer Bundesausschuss
GA	Generalanwalt
GebrMG	Gebrauchsmustergesetz
GG	Grundgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht
GRUR-RR	GRUR Rechtsprechungs-Report
Health Care Anal	Health Care Anual
IDPL	International Data Privacy Law
IIC	International Review of Intellectual Property and Competition Law
IFG	Informationsfreiheitsgesetz
internat.	International

IPR	Internet Policy Report
JDM	Judgment and Decision Making
JIPITEC	Journal of Intellectual Property, Information Technology and Electronic Commerce Law
JZ	Juristenzeitung
K&R	Kommunikation & Recht
LG	Landgericht
lit.	littera
MMR	MultiMedia und Recht
NJW	Neue Juristische Wochenschrift
NJW-RR	NJW-Rechtsprechungs-Report
Nr.	Number
NZA	Neue Zeitschrift für Arbeitsrecht
OLG	Oberlandesgericht
p.	page
para	Paragraph
PatG	Patentgesetz
p.m.a.	post mortem auctoris
Rec.	Recital
RefE	Referentenentwurf
RegE	Regierungsentwurf
RL	Richtlinie
Slg.	Sammlung der Entscheidungen des Gerichtshofs der Europäischen Gemeinschaft (Jahr und Seite)
sog.	sogenannte/sogenannter/sogenannten
TDDDG	Telekommunikation-Digitale-Dienste-Daten-schutz-Gesetz
TMG	Telemediengesetz
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
URL	United Resource Locator
Urt.	Urteil
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	versus
VerlG	Gesetz über das Verlagsrecht
VG	Verwertungsgesellschaft

WWW	World Wide Web
ZGE	Zeitschrift für Geistiges Eigentum
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUM-RD	ZUM-Rechtsprechungsdienst

Introduction

The notion that *knowledge is power* can be updated to *data is power* for the current times. Data is considered one of the most powerful assets in today's economy.[1] It enables personalised experiences, predictive analytics, and competitive advantages for businesses.[2] Cloud technologies have made it easier to store and access large amounts of data across multiple devices, and technologies such as artificial intelligence (AI) and machine learning are now capable of analysing large datasets to make predictions, provide personalised services, and automate tasks.[3] The growth of digital technologies has especially led to a massive increase in the amount of personal data generated and collected.[4] From social media interactions and online shopping to smart devices and wearable tech, individuals produce vast amounts of data daily. While there is much potential in those developments, significant privacy and ethical concerns have also been raised. These concern questions of transparency,[5] informational self-determination,[6] data

---

[1] *OECD*, Data-Driven Innovation, 179-186; *Sun/Yuan/Li/Zhang/Xu*, 70 Management Science 2023, 2645, 2645f; *Hacker*, Datenprivatrecht, 51; *Zuboff*, Surveillance Capitalism, 277-317; *Goldhammer/Wiegand*, Verbraucherdaten, 6; *Szczepański*, Briefing: Is data the new oil?, 1.

[2] *Sun/Yuan/Li/Zhang/Xu*, 70 Management Science 2023, 2645, 2645f; *Acquisti*, EC '04, 21, 21ff; *Galperti/Levkun/Perego*, 91 REStud 2023, 1007, 1007ff.

[3] *Hacker*, 55 Common Mark. Law Rev. 2018, 1143, 1144ff; *Armbrust and others*, 53 Commun. ACM 2010, 50, 51; *Buyya and others*, 25 FGCS 2009, 599, 601; *Goodfellow/Bengio/Courville*, Deep Learning, 5-7.

[4] *Hacker/Petkova*, 15 NJTIP 2017, 1, 4-6 *Zuboff*, Surveillance Capitalism, 15-20; *Manyika and others*, Big data, 1.

[5] *Reidenberg/Bhatia/Breaux/Norton*, 45 J. Leg. Stud. 2016, 163, 163ff; *Pollach*, '50 Commun. ACM 2007, 103, 105; *Zimmer*, Streamingplattformen, 10.

[6] *RouvroyPoullet*, in: Reinventing Data Protection?, 45, 58-61; *Lynskey*, The Foundations, 94-99; *Frosio*, 5 Colo. Tech. LJ 2016, 307, 313ff; Schwartmann/Jaspers/Thüsing/Kugelmann / *Leutheusser-Schnarrenberger,* 'Art. 17' DSGVO, para

security,[7] loss of control,[8] and even the manipulation of individuals.[9]

Individuals have become more aware of how their data is collected, used, and potentially misused.[10] This awareness is, however, often paired with a feeling of lack of control or even helplessness over managing their digital presence.[11] In the same way in which technological developments have led to these concerns, they might also offer certain means to alleviate some of those issues. For almost 10 years now, the use of so called Personal Information Management Systems (PIMS), which promise to empower users to control the collection and sharing of their personal data, has been debated.[12] These tools may come in different forms such as, for example, (1) data vaults or stores, which are secure environments where users can store their personal data and manage access by different service providers;[13] (2) consent management

---

6; *Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 556; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 60.

[7] *Bufalieri and others*, IEEE 2020, 75, 75ff; *Scudiero*, 3 EDPL 2017, 119, 124-125; Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 20' DSGVO, para 72.

[8] *Clifford/Graef/Valcke*, 20 GLJ 2019, 679, 685ff; *Soh,* 5 EDPL 2019, 65, 65f.

[9] *Denga*, 3 ZfDR 2022, 229, 230; *Weinmann/Schneider/vom Brocke,* 58 Bus Inf Syst Eng 2016, 433, 434f; *Nouwens and others*, CHI '20, 1, 2; *Waldman*, 31 Current Opinion in Psychology 2020, 105, 107.

[10] *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509, 509f; *Madden and others*, Pew Research Center 2015, 2, 5; *Caton/Haas*, 56 ACM Comput. Surv. 2024, 1, 2.

[11] *Clifford/Graef/Valcke*, 20 GLJ 2019, 679, 685ff; *Soh,* 5 EDPL 2019, 65, 65f.

[12] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht, 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[13] *Lehtiniemi*, 15 S&S 2017, 626, 626ff; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

tools, which help users to manage their consent given to various digital services;[14] or (3) digital assistants such as "data dashboards" or "data cockpits" which allow users to navigate their data rights and privacy settings across different platforms.[15] Still, many technical and legal questions continue to be open when it comes to the implementation of these technologies.

One crucial aspect, which is not yet resolved, relates to the question of controllership and liability in those tools. The Opinion on Personal Information Management Systems of the European Data Protection Supervisor mentions the necessity for a determination but does not provide a resolution, simply stating that *"it will be essential to clarify roles, responsibilities and liability"*.[16] There is also no unified approach within the market or academic literature, with only few publications explicitly dealing with the subject and businesses opting for various solutions.[17] The question of the roles taken by PIMS under the General Data Protection Regulation (GDPR) is, however, not a purely theoretical one. The designation of one of these roles has significant practical consequences on the obligations for providers and the safeguards they need to implement, as well as the extent of their liability.[18] This directly affects the level of protection guaranteed for the individual user, thereby making it a pivotal element in the context of data privacy. It seems crucial, therefore, to transparently and clearly define the roles taken by PIMS in order to

---

[14] *Datenethikkommission*, Gutachten, 133.

[15] *Attoresi/Moraes*, TechDispatch #3/2020, 3; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024).

[16] *EDPS*, Opinion 9/2016, para 45.

[17] *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356, 364-380; *Santos and others*, in: Privacy Technologies and Policy, 47, 47ff. For designations selected by the providers themselves refer to Part 2 Chapter 4: A. II. 3. Current Practice; C. I. Existing Service Offerings; D. II. 1. B) aa) Existing Offerings and II. 5. a) Existing Service Offerings.

[18] For details on the consequences of designating each role see Part 2 Chapter 3: A. VI. Effect; B. III. Effect; C. IV. Effect; B. I. 1. Relevance and D. II. 2. Relevance.

avoid further legal uncertainty and potential damages, not only to the individual user but to the concept of PIMS as a whole.

This thesis deals with these questions, and more specifically: Which role will Personal Information Management Systems take under the GDPR? Should they be considered a data controller, processor, joint controller, or a third party? And what are the consequences of these designations for the data subject? To this end, Part 1 will at first define the term PIMS and then provide a general overview of the currently existing types of service offerings available on the market. Part 1 will furthermore analyse to what extent these tools are in fact able to support the data subject in exercising their rights, as well as provide suggestions for further developments. Part 2, which constitutes the main section of this thesis, will begin with defining the roles which could, in principle, be taken by the parties under the GDPR. In the second section, the types of service offerings identified in Part 1 are then analysed based on those definitions and the different roles taken by those are defined. As a result of that analysis, several risks to the rights and freedoms of the individual are identified. These relate predominantly to the diverging and often even contradictory roles taken by providers for various elements of the service. Based on these findings, Part 3 strives to find solutions, leading to more consistency, as well as legal protection for the individual user. Thus, a more restrictive definition for PIMS is suggested. As a next step, alternative forms of liability outside of the GDPR are explored. Finally, alternative forms of interpretation within the GDPR are considered with the goal of ensuring the highest level of protection for the data subject. At the same time, the suggested solutions would also lead to more legal certainty for providers and therefore, by extension, to more developments within this field.

Part 1

A New Hope

User Centric Privacy through Personal Information Management Systems

The focus of this thesis lies in the analysis of the respective functions fulfilled by Personal Information Management Systems under the General Data Protection Regulation, including the extent of their responsibilities and liabilities. As a first step, it is therefore necessary to define what types of tools and service offerings would fall under this term. Part 1 will provide an in-depth analysis of the terminology. It will also, to a greater extent, focus on examining the potential of these systems to support the individual person in the exercise of their rights under the GDPR. For that purpose, both existing functionalities and those which are currently under development will be investigated. Where the current market realities do not seem to focus on the support of a certain right, considerations for future advancements shall also be included.

Chapter 1

Terminology

In order to begin an analysis of Personal Information Management Systems and, in particular, what role such a system will take vis-a-vis the data subject, it is crucial to define what constitutes a Personal Information Management System. The term itself has actually existed longer than the GDPR and even most other data protection laws because outside of the realm of information privacy, it is being used for several tools and services that in fact have little or nothing to do with the subject of this thesis. It is therefore crucial to look at the various meanings attached to this denomination in order to define the perimeters for this thesis.

A. Alternative Contexts

As a starting point, general conceptual contours will therefore be established, as well as a delineation of the systems which fall outside of the scope of the presented analysis.

I. Organisers

Personal Information Management is traditionally described as how an individual creates, acquires, stores, organises, distributes and retrieves information.[1] The term "Personal Information Management Systems" is therefore commonly used to describe tools which facilitate these actions, such as storage and organisation of data and searching through databases based on various criteria, as well as

---

[1] *Jones and others*, in: Encyclopedia of Library and Information Sciences, 3584-3605; *Teevan/Jones/Bederson*, 49 Commun. ACM 2006, 40, 40; *Al Nasar/Mohd/Mohamad Ali*, in: IEEE 2011, 197ff; *Lodato*, CHI EA '04, 810, 810ff.

the coordination of meetings, deadlines, tasks, and personal contacts. For this reason, these tools can broadly be referred to as "organisers" as their functionalities are primarily focused on the management of either existing datasets (cataloguing and classification), as well as the personal aspects of an individual's everyday life (task and contact management).
A large part of the function of Personal Information Management Systems, in that sense, is actually concerned with the retrieval of information. Finding a specific item out of large databases is one of the biggest challenges in today's information management.[2] Based on that, all sorts of browsers and search engines would be included in the definition, covering anything from a basic search functionality in a library database to an internet browser.
The second large group of these so called "organisers" incorporates functionalities such as task management, personal archiving, and contact management.[3] These tools make up, to a large extent, a form of personal organiser and can come as e-mail and note taking programs, calendars, or address books, with most of these applications covering a range of tasks and often connecting with each other in various constellations.[4]

II. Human Resources

The second meaning which, however, is used significantly less and predominantly in corporate settings rather than academia, refers to the area of human resource management. Herein the term "Personal Information Management System" is used to describe tools

---

[2] *Bergman/Beyth-Marom/Nachmiasi/Gradovitch/Whittaker*, 26 ACM Trans. Inf. Syst. 2008, 1, 1ff; *Voit/Andrews/Slany*, in: Personal information intersections, 60, 60; *Dumais and others*, 49 SIGIR Forum 2016, 28, 28; *Al Nasar/Mohd/Mohamad Ali*, in: IEEE 2011, 197.

[3] *Whittaker/Bellotti/Gwizdka*, 49 Commun. ACM 2006, 68, 68f; *Whittaker and others*, 11 ACM Trans. Comput.-Hum. Interact. 2004, 445, 445ff.

[4] *Whittaker/Bellotti/Gwizdka*, 49 Commun. ACM 2006, 68, 70-73; *Bauer*, 1 Young Information Scientist 2016, 45, 46.

which support the work of HR-professionals in handling the vast amount of personal data of the company's employees. The functionalities of such systems can range from monitoring work attendance, leave management and payroll administration, through to performance reviews, as well as completed trainings, achievements, and other forms of evaluations of the employees' competences and productivity.[5]

The terminology can actually become even more confusing when considering the German language as the word "Personal" means "staff" (or "personnel") and the phrase "Personalinformationssysteme" ("Personnel Information Systems") is very commonly used in human resources management tools. It is also found even in literature regarding data protection[6] and official guidelines by the Federal Commissioner for Data Protection and Freedom of Information.[7] It is therefore important to differentiate that while these types of systems are the subject of many publications and discussions within the field of data privacy and can in fact be used to a certain extent to protect the rights and freedoms of the data subject, they are not being analysed as part of this thesis. Such an analysis regarding the questions of controllership and liability would be unnecessary; as with any human resources management system, the employer will always be considered the controller, as the responsibility for the processing activity is naturally attached to this role.[8]

---

[5] *Mann/Parab/Sankpal/Morde*, 4 IJSER, 2013, 681, 681 ff; *Alves e Silva/da Silva Lima*, in: Manag. of Info. Sys.; *Dorel/Bradic-Martinovic*, in: Labour Markets and Human, 25, 33-36; *Navarro*, 8 IJSR 2019, 1826, 1826.

[6] *Däubler*, Gläserne Belegschaften, 52-55; *Gola/Wronka*, HandB zum Arbeitnehmerdatenschutz, para 809, 1436 and 1554; *Wedde*, Automatisierung im Personalmanagement, 4f, 14, 22-25, 30, 35, 37, 46.

[7] *BfDI*, Leitfaden Personalrat, 4; *BfDI*, 23. Tätigkeitsbericht, 62 and 127.

[8] *EDPB*, Guidelines 07/2020, para 27.

III. Compliance Management

Last but not least, the consistent rise in attention given to the subject of data privacy in general and, more specifically, compliance with the GDPR since its coming into effect in 2018, has led to a large amount of compliance tools being developed which are mainly aimed at supporting companies in demonstrating their adherence to the Regulation in accordance with the principle of accountability, set forth in Art. 5(2) of the GDPR.[9] Many of those in their marketing describe themselves as "PIMS", with the terms "Personal Information Management System", "Privacy Information Management System", and "Data Protection Management System" basically being used interchangeably.[10] The functionalities of these can basically cover any of the requirements set by the GDPR but mostly focus on the creation and maintenance of the record of processing activities, the performance of Data Protection Impact Assessments, the documentation and reporting of breaches, the handling of data subject requests, and third party management.[11]

In a sense, these tools are actually very close to the meaning of Personal Information Management Systems which will be analysed subsequently in this thesis, as generally they are trying to achieve the same purpose: conformity with the General Data Protection Regulation and by extension, the protection of the rights and freedoms of individuals. Similarities can also be seen in the functionalities,

---

[9] *Jung*, 5 ZD 2018, 208, 208ff.

[10] As of April 2026 the use of the term "Personal Information Management System" of "Data Protection Management System" in their marketing can be seen with the following providers: PiwikPro, https://piwikpro.de/glossar/pims-personal-information-management-systeme/) (accessed: 14 April 2026); Impelsys, https://www.impelsys.com/gdpr/ (accessed: 14 April 2026); One Trust https://www.onetrust.com/solutions/iso27701/ (accessed 14 April 2026); Privacy Pilot, https://www.scheja-partner.de/leistungen/datenschutz-management-system.html (accessed 14 April 2026).

[11] An exemplary overview of various providers, including a description of their functionalities can be found in: https://iapp.org/media/pdf/resource_center/2022TechVendorReport.pdf (last accessed: 17 April 2026).

which, particularly in the areas of consent management and the facilitation of data subject requests, will basically mirror each other. It is, however, of utmost importance to remember that PIMS in the sense of compliance tools are primarily focused on the support of the controller in adhering to the legal requirements they are subject to, not the support of the individual. While for marketing purposes, providers of data protection management solutions might also refer to the many benefits which occur on the side of the data subject, such as better transparency, easier access or heightened security, none of these are the main purpose of the tool and this will be reflected in the way the features are set up. In the end, the paying customer for a Data Protection Management System is the data controller and the interests of this entity will most likely take preference to those of the individual. Another crucial difference, which also needs to be pointed out, is that while these tools might make it easier for the data subject to act on their rights as their request will be processed more efficiently by the data controller, they are in the end not the ones managing those, as the system, together with all its functionalities, will still be predominantly administered by the data controller. This set-up, while potentially serving similar objectives, is completely contrary to the explicit purpose of user-centric Personal Information Management Systems, which are supposed to give the individual person control over the management of their personal data (see Part 1 Chapter 1: B. Context of the Thesis).

The source of this somewhat confusing wording, where two different types of systems with functionalities which are to an extent very similar or may even mirror each other, is actually most likely to be found in the wording chosen by national, as well as international standards bodies. In August 2019, the International Organization of Standardization (ISO) published the ICO/IEC 27001:2019, which is a privacy extension to ISO/IEC 27001 and ICO/IEC 27002 specifying the requirements for establishing, implementing, and maintaining a Privacy Information Management System.[12] Similarly, the British

[12] https://www.iso.org/standard/71670.html (accessed 14 October 2024).

Standards Institution (BSI) published in March 2017 their BS 10012:2017 and updated it in July 2018 to BS 10012:2017+A1:2018, which is a standard specifying the requirements for Personal Information Management Systems in the sense of organisational frameworks for assuring compliance with data protection laws and good practice.[13] Given the nomenclature used by these standards bodies, it is easy to see why the providers of compliance tools might refer to their offerings as "PIMS", especially if their product is in fact certified under one of those standards or if they offer help in achieving such as part of their service.[14] For the reasons described above it is, however, essential that these types of systems are clearly separated from the subject of this thesis, which is why from this point on, organisational compliance tools and structures will be referred to as Data Protection Management Systems (DPMS).

B. Context of the Thesis

While as of the time of writing no uniform definition existed for PIMS, the central focus for our purposes will be the meaning established by the European Data Protection Supervisor in the Opinion 9/2016 on Personal Information Management Systems. Here they are described as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*.[15] This understanding with slight variations also seems

---

[13] https://knowledge.bsigroup.com/products/data-protection-specification-for-a-personal-information-management-system?version=standard (accessed: 26 February 2026).

[14] See for example: https://www.onetrust.com/solutions/iso27701/ (accessed 26 February 2026).

[15] *EDPS*, Opinion 9/2016, para 4.

to have been predominantly accepted within the literature on the subject.[16]

The central idea of such systems lies in the understanding that users should be given the means to determine how their personal data is handled.[17] This idea is clearly supported in Recital 7 of the GDPR which states that *"[n]atural persons should have control of their own personal data"*. While it might seem obvious that each individual should be able to be in charge of their own data and identity, it has long been established that this is not the case under the current framework in which our digital society operates.[18] People report feeling confused and unsure about what happens to their data, as well as helpless in attempting to understand the complicated processing operations and transfer set-ups created by companies.[19] This general feeling of helplessness or inability to change existing conditions is also a direct result of the power imbalance between the business and the customer, where the first can easily control how and when certain information is given, while the latter often finds him- or herself feeling pressured into making a fast decision or are simply left with a "take it or leave it" approach.[20] It is precisely this asymmetry within

---

[16] *Schwartmann/Weiß (eds.),* 'Datenmanagement- und Datentreuhandsysteme', https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht, 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[17] *EDPS*, Opinion 9/2016, para 4; *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

[18] *Blume*, 2 IDPL 2012, 26, 29; *Tolmie and others*, 'CSCW '16, 491, 491ff; https://arxiv.org/abs/1811.08660v1 (accessed 02 March 2026); *EDPS*, Opinion 9/2016, para 1.

[19] *Clifford/Graef/Valcke*, 20 GLJ 2019, 679, 685ff; *Soh,* 5 EDPL 2019, 65, 65f.

[20] *Christl*, Corporate Surveillance, 31, 85; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-

the power structure that Personal Information Management Systems try to rectify by supporting the data subject in the enactment of their rights and freedoms.

It should also be noted that while PIMS have the potential to support companies in their assurance of GDPR compliance as, for example, proving the validity of consent obtained via such a tool would most likely be easier than under the current regime, this is not their primary goal and will therefore not be the focus of this chapter. The interests of the data recipients or other actors involved in the operation will, however, be crucial when determining the respective roles and responsibilities vis-a-vis the data subject, in particular whether their position is defined as a controller, processor, or neither. In that context, the interests of the business will therefore also need to be considered to the extent that they affect the identification of the parties engaged in the determination of the means and purposes of the processing of personal data at hand. This analysis will, however, be concluded in Part 2 Roles taken by Personal Information Management Systems under the GDPR, while the next Part 1 Chapter 2: Classification will place its focus on providing an overview of the possible functionalities and how each of those support the data subject's rights as outlined by the General Data Protection Regulation.

---

und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *EDPS*, Opinion 9/2016, para 4.

Chapter 2

Classification

In the same vein in which there is no official definition of what constitutes a Personal Information Management System, there is also no uniform understanding of the functionalities such a system would need to offer in order to fall under that definition, other that the fact that it should *"empower individuals to control the collection and sharing of their personal data"*. Since the idea of creating such systems is still relatively new and the market for such has only in the last decade picked up in speed, there was simply not enough time for any sort of homogenous standards to develop.

Due to this fact, the term "PIMS" is actually used for a large variety of existing, or at this point, often still theoretical service offerings. These include many functionalities in diverse constellations and combinations which all follow the purpose of giving data subjects more control over their data, but in very different ways. Adding to the overall confusion is the fact that this wide range of service offerings also comes with an assortment of denominations, such as, for example: personal data spaces, stores and vaults,[21] privacy management tools,[22] data dashboards,[23] data boxes,[24] data cockpits,[25] and many more. These are at times used interchangeably, while at other times in order to differentiate between each other.

---

[21] *Lehtiniemi*, 15 S&S 2017, 626, 626ff; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

[22] *Datenethikkommission*, Gutachten, 133.

[23] *Attoresi/Moraes*, TechDispatch #3/2020, 3.

[24] *Crabtree and others*, 4 J Reliable Intell Environ 2018, 39, 39ff.

[25] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?blob=publicationFile&v=1 (accessed: 12 October 2024).

For this analysis, it is therefore necessary to not only describe the functionalities of PIMS, but also to structure them in order to provide a comprehensive and logical overview. The following section establishes some general categories based on the systems' objectives, as well as the technical set-up. The outlined components have been divided into I. Storage, II. Information, III. Consent, and IV. Requests. The first three sections focus on the assurance requirements which automatically apply to any controller, while the fourth analyses the various forms of obligations which arise based on a request made by the data subject. Focus will also be put on the question of how each of these components strengthen the protection of the individual's data, with a particular emphasis on the rights of the data subjects, as laid down in Chapter III of the GDPR and the general principles of processing personal data, established in Article 5. It should, however, be kept in mind that these categories solely constitute a convention asserted for the purpose of this thesis and in no way reflect an actual classification present in the market.

A. Storage

The operation of any Personal Information Management System will require the storage of personal data. While secure storage in and of itself can be considered a privacy enhancing service, it will most often be accompanied by other offerings such as data sharing, organisation, and password management.[26] It is, however, still interesting to review separately because of its crucial effect on the integrity and confidentiality of the data, as well as the central question of the data location.

---

[26]See for example: Data Vaults, https://www.datavaults.eu/ (accessed: 25 February 2026); Cozy Could, https://cozy.io/en/ (accessed: 25 February 2026); Nextcloud, https://nextcloud.com/ (accessed: 25 February 2026); Meeco, https://www.meeco.me/ (accessed: 25 February 2026).

I. Technical Architecture

The primary distinction regarding the technical architecture of Personal Information Management Systems lies in the question of whether data is being stored locally or within the cloud.

1. Local Storage

Local storage means that all data is physically kept within the user's device such as a smartphone, computer, or even completely separate hardware.[27] In this model, the data is kept on the device in an encrypted form and developers would have to interface though the hardware-provider's Application Programming Interface (API) in order to gain access.[28] While this would probably be considered the golden standard when it comes to the question of user-centricity, there are multiple downsides which currently prevent these types of solutions from dominating the market.

First, if such a solution was actually to be used in order to manage the entirety of one's personal information (which at the moment is not really a viable option, but does seems to be a direction in which, at least in theory, the systems do in fact want to develop), then this would require a large amount of storage space within the device in question. Second, local storage raises several security concerns since the developer would only have limited options in controlling the level of protection. In most instances, everyday technical appliances such as phones, laptops or tablets are solely protected by very simple passwords so there would be a very high risk of someone gaining access to the user's personal data without the data subject's agreement. There are certain technical measures that could be taken in order to remediate this risk at least partially, such as physical separation of the encryption and decryption key, through the use of a third

---

[27] See for example: Freedom Box, https://freedombox.org/about/ (accessed: 25 February 2026).

[28] *Brochot and others*, PDS, 20.

party verification service.[29] This set-up, however, is not only complicated but most of all costly and with no other economic incentive on the side of the provider (such as being able to access and use the data for their own purposes) would most likely lead to an expensive and thereby commercially unsuccessful offering, which might explain why cloud storage solutions are effectively dominating the market.[30]

2. Cloud Storage

The many advantages of cloud storage are well known. While it is, as of now, the most cost effective and convenient method of storing data, there are, however, many aspects that need consideration before deploying such a solution, especially when it comes to hosting personal data. There are various forms of cloud storage, all which of which come with their own list of advantages and disadvantages. There are three main types of clouds that are most commonly used: public, private, and hybrid.[31]

a) Public Cloud

Public clouds are provisioned for open use by the general public and are usually provided by large vendors which take over the deployment and maintenance of the servers.[32] Examples include Amazon Web Services, IBM, Google Cloud, and Microsoft Azure. In this solution, the infrastructure is usually shared between clients, which means that they might use the same hardware and have their data stored in the same database.[33] Typically, a public cloud is the easiest

---

[29] *Brochot and others*, PDS, 21.

[30] COM, An emerging offer of "personal information management services" - Current state of service offers and challenges, 10.

[31] *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 38; *Yang/Xiong/Ren*, 8 IEEE Access 2020, 131723, 131724.; *Galloway*, A cloud architecture, 4.

[32] *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 38f; *DSK*, Cloud Computing, 7; *Mell/Grance*, The NIST, 3; *Schröder/Haag*, 4 ZD 2011, 147, 148.

[33] *Hon/Hörnle/Millard,* 26 Int. Rev. Law Comput. Technol. 2012, 129, 130.

to deploy as it requires little to no work on the side of the enterprise. It also provides the easiest option to access data and the fact that these are typically standardised service offerings makes it likely to be the most cost effective.[34] The easy access resulting from a lower level of administrative controls, while convenient and possibly desired for certain service offerings might, however, pose an enormous security risk. This can become problematic as public clouds typically offer very little options of customisation, making it difficult to add any additional security layers. Therefore, the use of a public cloud for implementing a Personal Information Management System does not seem to be a viable solution and if it was to be considered, would need to be examined with much scrutiny and vigilance.

b) Private Cloud

In a private cloud, the infrastructure is provisioned for exclusive use by a single organisation and the data is usually stored over the company's intranet and protected by its own firewall.[35] Also, the management and maintenance of the servers needs to be taken over by the internal IT staff of the hosting enterprise.[36] This solution, if managed correctly, definitely ensures the highest level of security. It will, however, also cause an exponential rise in costs especially since expert staff need to be engaged in order to ensure that the desired level of security can not only be established but also maintained.[37] While the increase in expenses is to be considered especially for enterprises aiming at the realisation of profits, a lack in security for a service explicitly trying to assure the protection of the rights and freedoms of the data subject would simply not be acceptable and could therefore not be considered a viable business model. Regardless of the actual level of security, the preference of the customer, as well

---

[34] *Yang/Xiong/Ren*, 8 IEEE Access 2020, 131723, 131724.

[35] *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 38; *DSK*, Cloud Computing, 7; *Mell/Grance*, The NIST, 3; *Schröder/Haag*, 4 ZD 2011, 147, 148.

[36] *Yang/Xiong/Ren*, 8 IEEE Access 2020, 131723, 131724.

[37] *Galloway*, A cloud architecture, 5.

as their level of trust, also needs to be factored in. The reason many are looking for secure storage solutions is precisely the fact that they do not trust the offerings of the large commercial providers available on the market. One would therefore be very ill advised to attempt costs savings in this area. The Personal Information Management Service providers, offering storage as part of their business model, have also taken this approach, opting for private cloud storage, rather than public.[38]

c) Hybrid Cloud

Last but not least, there are hybrid cloud storage solutions available which constitute a combination of the latter two, wherein the services from both domains are integrated with each other and the company enters a more extensive relationship with the external service provider in order to facilitate their needs.[39] Companies opting for this model will typically classify datasets in accordance with their sensitivity and level of confidentiality, and then store these in higher protected, private storage facilities while keeping non-critical information in the lower-cost public cloud.[40] While choosing this model would definitely make sense for small and medium-sized business who are processing sensitive information to a certain extent but would not have the means to finance a fully operable private cloud for all of their data, it is again unlikely to make sense for a provider of Personal Information Management System, especially if data storage is part of their service offering. The enterprise in question could store their

---

[38] See for example: Data Vaults, https://www.datavaults.eu/ (accessed: 25 February 2026); Cozy Could, https://cozy.io/en/ (accessed: 25 February 2026); Nextcloud, https://nextcloud.com/ (accessed: 25 February 2026); ownCloud, https://owncloud.com/ (accessed: 25 February 2026); Meeco Vault, https://www.meeco.me/ (accessed: 25 February 2026).

[39] *DSK*, Cloud Computing, 7; *Hon/Hörnle/Millard,* 26 Int. Rev. Law Comput. Technol. 2012, 129, 130.; *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 39; *Mell/Grance*, The NIST, 3; *Schröder/Haag*, 4 ZD 2011, 147, 148.

[40] *Yang/Xiong/Ren*, 8 IEEE Access 2020, 131723, 131724.

business data, such as transactional histories, tax statements, marketing strategy, or internal communications on public cloud servers. Whether that is, in fact, advisable is a completely different question but since the subject of this analysis are is PIMS in the context of supporting data subjects in regaining control over their data, how a company handles their business information is irrelevant.

Regarding the users' data, however, a hybrid model in which data would in part be stored in a private and in part in a public cloud, does not seem to be a feasible solution for multiple reasons. First, the question arises as to who would perform the classification of the sensitivity of the data. Having this done by the provider would potentially constitute a large interference in the data subject's private life and most likely not be considered proportional to the pursued aim. On the other hand, having the data subject itself make that decision might work better from a data protection standpoint and would definitely be in line with the idea of strengthening the individual's influence over what happens with their data. However, it would also most likely not lead to objective results, as the individual's subjective feelings will, even unconsciously, dominate the decision-making process. It might also provoke the same "decision making fatigue" which has been observed with respect to privacy notices and cookie banners (see Part 1 Chapter 2: C. III. 4. Consent Fatigue). In turn, the individual might simply start automatically listing all of their data on the private server, not only defeating the entire purpose of the hybrid model but also ultimately creating a negative user experience.

II. Storage Location

Location, location, location... The old real estate wisdom definitely holds true for the data privacy landscape of the 2020's. The question where data is physically stored has always required consideration, not only from a data protection but also an information security perspective. Transatlantic data flows have been a source of contention

for a long time.[41] The Schrems II[42] judgement has certainly amplified that and has not only caused major changes within the field, but has also brought the question of international data transfers to the forefront of the discussion.[43] While the topic has always been one of the classics for data protection professionals, it was not until the judgement that it entered into the general consciousness in such a profound way.[44]

Whereas the post Schrems II landscape, in which storage of personal data with US cloud providers become a major issue for concern, has been an enormous headache for legal departments all over the world, it incidentally has also been an immense support for the development and rise of intra-European cloud storage providers, hosting and processing their data exclusively within the European Economic Area. Unsurprisingly, most of the Personal Information Management Systems on the market or under development also opt

---

[41] *Bräutigam*, in: Data Protection, Privacy and European Regulation in the Digital Age, 143, 143ff; *Maldoff/Tene*, 17 Colo. Tech. L.J. 2019, 295, 295ff; *Schwartz*, 80 Iowa L. Rev. 1995, 471, 471ff.

[42] Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559.

[43] *Breitbarth*, 7 EDPL 2021, 539, 539ff; *Hallinan and others*, 29 Eur J Hum Genet 2021, 1502, 1502ff; *Etteldorf,* 20 ZD-Aktuell 2021, 05552; *Golland*, 36 NJW 2020, 2593, 2593 ff; *Kipker*, 8 ZD 2021, 397, 397f.

[44] https://www.sueddeutsche.de/wirtschaft/datenschutz-schrems-ii-europaeischer-gerichtshof-eugh-allianz-gdv-hannover-rueck-1.5481309 (accessed: 05 March 2026); https://www.faz.net/pro/digitalwirtschaft/nach-schrems-urteilen-ist-ein-sicherer-datenfluss-in-die-usa-unmoeglich-17350923.html (accessed: 04 March 2026; https://www.theregister.com/2021/11/24/max_schrems_files_corruption_complaint/, accessed 25 February 2026; https://www.cnbc.com/2021/04/19/privacy-shield-eu-officials-pushing-hard-for-us-data-sharing-pact.html (accessed: 15 April 2026).

for sole data storage within the EU,[45] with some of them explicitly advertising their superiority over US-based companies.[46]

While exclusive intra-European storage and processing can certainly be seen as the gold standard, it should not be considered a must. As long as all the requirements for third country transfers laid down in Chapter V of the GDPR are met, there does not seem to be any reason not to store data outside of the EEA, especially if this, together with all of its implications, is transparently communicated to the data subject. Sometimes storage outside European jurisdictions might even be in the interest of the individual, as there are also those who are concerned about the surveillance activities of European Government Agencies. Since July 2023, enterprises may also certify under the new EU-US Data Privacy Framework, for which an adequacy decision has been issued by the European Commission.[47] Its longevity however is questionable considering that the European Centre for Digital Rights, noyb, has already announced plans for taking legal action against it.[48]

Whereas data storage within a third country should therefore be possible, the prerequisites for its legality should not be discussed at

---

[45]See for example: Data Vaults, https://www.datavaults.eu/ (accessed: 25 February 2026); Cozy Could, https://cozy.io/en/ (accessed: 25 February 2026); Nextcloud, https://nextcloud.com/ (accessed: 25 February 2026); ownCloud, https://owncloud.com/ (accessed: 25 February 2026); Meeco Vault, https://www.meeco.me/ (accessed: 25 February 2026).

[46]The following passage is an example lifted from the webpage of 'ownCloud': *"German server centres are subject to German law, ensuring providers have no obligation towards any authority requesting disclosure or access to data (as opposed to US-based providers for example, who are subject to the CLOUD-Act). Even in case of a presumed criminal offence, German authorities only have limited access to your data. However, these conditions only apply to providers with both their company and server location in Germany. Only ownCloud Online offers you this: where protection of your data is concerned we make no compromises."*, https://owncloud.online/gdpr-compliance/ (accessed: 02 March 2026).

[47]European Commission, Adequacy decision for the EU-US Data Privacy Framework (10 July 2023).

[48]https://noyb.eu/de/european-commission-gives-eu-us-data-transfers-third-round-cjeu (accessed: 02 March 2026).

this point. The requirements for such transfers take up an entire Chapter of the GDPR alone and are, as mentioned above, the subject of many publications and controversy and would certainly provide enough material for a separate thesis altogether. Because there are, however, some US-based providers of Personal Information Management Systems,[49] as well as stakeholders who are based in Europe and use subcontractors from the States,[50] we should at least take a quick look at the potential legal issues resulting from such a set-up.

1. US-Based PIMS Providers

The existence of US-based providers of Personal Information Management Systems, if such were to be used by data subjects residing in Europe or send data subject requests to European businesses, raises several questions. This is mainly the case since PIMS would most likely fall under the definition of an "electronic communications service provider" in the meaning of section 702 of the Foreign Intelligence Surveillance Act.[51] Data transfers to such entities are, however, generally not considered as compliant with the GDPR. The Court of Justice of the European Union found that both FISA and E.O. 12333 cannot be regarded as limited to what is strictly necessary and thereby are not in line with the principles of proportionality and data minimisation.[52] This does not constitute a problem in itself, as a US-based provider of services such as secure storage solutions, breach monitoring, consent, or deletion request management falls solely under the respective US Federal or State privacy laws. Such

---

[49]For example: My Data Can, https://mydatacan.org/ (accessed: 14 April 2026); Privacy Bee, https://privacybee.com/ (accessed: 14 April 2026).

[50]For example, as of October 2024 CozyCloud uses the following US service providers: MailChimp (in order to send product marketing e-mails), Helpscout (in order to host user documentation and answer support e-mails), Product Board (in order to group feedback from users) and Trello (in order to prioritize user bugs), https://cozy.io/en/privacy/ (accessed: 14 October 2024).

[51]*Vladeck*, Expert Opinion, 3-5.

[52]Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559, para 184f.

an entity might, however, also be subject to the GDPR in accordance with Art. 3(2)a) if such an offering was explicitly made to data subjects in the European Union. As per Recital 23, the mere accessibility of a website is not sufficient to ascertain such an intention. If, however, the entity was to use European languages on their website or mention European users, this could be construed as an offering of services to such. The same should also be assumed in instances where the website explicitly mentions support for data subjects in enacting their rights under the GDPR.[53]

If that were the case and the extraterritorial effect was in fact to apply, the PIMS provider would be subject to the GDPR and potentially enter a conflict with national law. Interestingly, it might also be more difficult for such an enterprise to prove the "essential equivalence" of their level of data protection, as the direct disclosure of personal data by the data subject to an entity established in a third country does not constitute a "transfer" in the meaning of Chapter V. Consequently, all the transfer mechanisms typically used to assure the existence of appropriate safeguards, such as standard data protection clauses or "transfer impact assessments", will not be available.[54] It might therefore be advisable to have the representative, designated in accordance with Art. 7 (1), liaise with the Data Protection Authorities, prior to entering the European market.

---

[53]For example, 'Privacy Bee' uses the following wording while describing their 'Features' „*Setup your **Trusted Companies** within the Privacy Bee platform and our team will fight to ensure your wishes are respected, even invoking any applicable privacy legislation to legally compel companies to comply (**GDPR, CCPA,** etc)*.", https://privacybee.com/features/proactive-data-privacy/ (accessed: 01 November 2024, suggesting a focus on the European market, but then however in their FAQs answers the question *„Does Privacy Bee work in Europe?"* with *„While we plan to quickly expand globally, today our focus is 100% on the US market"*, https://privacybee.com/faq/ (accessed: 01 November 2024) seemingly denying that fact.

[54]*EDPB*, Guidelines 05/2021, para 12; Wolff/Brink/v. Ungern-Sternberg / *Hanloser,* Art. 3 DSGVO, para 26b.

2. PIMS with US-Based Subsidiaries or Vendors

On the other hand, there might be providers of Personal Information Management Systems residing in the EU but either using US-subsidiaries or subcontractors for storage or other processing operations. Here, it is important to remember that mere access to data from a third country already constitutes a "transfer" under the GDPR.[55] This is actually very relevant as in practice, the vendor's data centres might often be physically located within the EEA but IT-support will most likely be provided from the US. These set-ups are also to be considered as third country transfers and all the general requirements for such apply equally. As cloud services also typically fall under the definition of "electronic communications service providers", data residing with them will also potentially be subject to surveillance under FISA and E.O. 12333 in the same vein as it would be simply lying with a US service provider. It should also be noted that the US government has previously, in other contexts, taken the position that a EU company with a US subsidiary would be subject to federal law, as the decisive element is whether data is in possession or control of a US communication service provider as defined in 50 U.S.C. § 1881(b)(4).[56] This means that reliance on the safeguards listed in Art. 46 (2) GDPR will most likely not be sufficient in order to assure an adequate level of protection and therefore additional measures would need to be applied.[57] Since, however, the effectiveness of such is still subject to much uncertainty and debate as well as scrutiny from the Data Protection Authorities, these should be carefully examined as part of a Transfer Impact Assessment which will consider all the specific circumstances of the transfer in question.[58]

---

[55] *EDPB*, Recommendations 01/2020, para 13; Ehmann/Selmayr, *Zerdick*, Art. 44, para 7.

[56] *Vladeck*, Expert Opinion, 9.

[57] Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559, para 134; *EDPB*, Recommendations 01/2020, para 23.

[58] *Sandfuchs*, 3 GRUR Int. 2021, 245, 247; *EDPB*, Recommendations 01/2020, para 28-43.

Even if the strict requirements for the engagement of US based subcontractors were to be met, there is also another point that requires consideration. The newly raised public awareness, regarding the potential consequences of such data transfers to the US which resulted from the extensive media coverage on the Snowden revelations, as well as the two Schrems cases, will make it very likely that data subjects based in the EU opting for a European provider of Personal Information Management Systems, will not look particularly fondly on the use of such vendors.[59] Any business model offering the storage of personal data will have to make a conscious and thought-out decision regarding the location of their data centres.

III. Security Measures

According to Art. 5(1)(f) GDPR, personal data should be *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".* This principle of integrity and confidentiality was actually not part of the main "principles relating to data quality" under the old Data Protection Directive,[60] which clearly indicates that the lawmakers wanted to underline the importance of such measures for the protection of personal data. Its denomination, however, does not really transpose the entire meaning as Art. 32 and Recital 39 clearly broaden the scope by including the objectives of availability and resilience, as well as the prevention of unauthorised use or access. Considering the con-

---

[59]This would also be another reason why the deployment of a public cloud, as discussed under Part 1 Chapter 2: A. I. 2. Cloud Storage, is most likely not the best option, since all of the primary providers (for example: Amazon Web Services, IBM, Google Cloud and Microsoft Azure) are US-based.

[60]Section II Article 6 No. 1 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

text, it can be assumed that the purpose of this principle is safeguarding the realisation of the other data protection principles though technical and organisational means.[61]

It should also be noted that assuring the security of personal data concerns not only its storage, but the entire life-cycle. This will be analysed at this point because of the paramount importance of security in the case of storage, as well as the fact that many general technical settings are actually taken at the storage system. The discussed objectives and measures, however, apply to the entire processing operation. The technical and organisational measures will therefore need to be carefully considered during the implementation of a Personal Information Management System and additionally serve as a first example of how PIMS can actually reinforce these primary principles and strengthen the rights and freedoms of the data subject.

1. Appropriateness

Article 32(1) of the GDPR specifies that the security measures required to be taken by the controller and processor should be selected *"[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons"* in order to assure a level of protection which is *"appropriate to the risk"*. It goes on the clarify in Paragraph 2 that the particular risks resulting from the processing in question need to be considered "…*in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed".*

This additional criterion of "appropriateness" can be seen as an extension of the principle of proportionality whereas its vagueness

---

[61] *Roßnagel* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 5 DSGVO, para 168.

most likely results from the concept of technological neutrality, enshrined in Recital 15, as well as the notion of the GDPR as a dynamic piece of legislation, where the specific requirements will progress jointly with technological developments.[62] While often the source of uncertainty among the controllers and processors as to what is in fact to be considered appropriate. it also gives them significant leeway in their selection, as well as vast room for interpretation.[63]

In this context, it should, however, be noted that the bar of what is being considered "appropriate" will be significantly higher for Personal Information Management Systems compared to most corporations or organisations. As per Art. 32(1), the purposes of processing are one of the factors to be accounted for when assessing a necessary level of security. Typically, an entity will process personal data as part of their business model, but exist primarily for the realisation of different goals. The purpose of the processing might therefore, be the sale of a product, the provision of a service, or compliance with some sort of legal obligation, for example. The difference between a provider of Personal Information Management Systems and other service providers such as e-commerce, consultancy, banking, health care, or real estate, is that the underlying purpose of these has little or nothing to do with the processing of personal data; the processing activities are simply a side effect, necessary for the achievement of other objectives. With PIMS, it is precisely the opposite, since their primary purpose is the support of the data subject in the realisation of their right by giving them the power to control their data. The purpose of the processing is therefore the protection of personal data itself. This is why for Personal Information Management Systems, the highest possible level of protection is to be considered "appropriate". And while, as per Art. 32(1), other factors such as the state-of-the art, the cost of implementation, and the severity and likelihood of

---

[62]Gola/Heckmann / *Piltz*, Art. 32 DSGVO, para 13-17; *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 20-22.

[63]Rücker/Kugler, *Dienst*, C. Lawful processing, para 350.

certain risk will still be taken into consideration, the basic level of security which is to be considered the starting point will need to be the leading and most advanced structural and technical configuration.

This expectation is also supported by the way providers of PIMS typically market themselves in statements such as *"[y]our privacy and the protection of your personal data guide our technological choices"*[64] or de *"supporting digital platforms to improve their digital services"*[65] or *"turning privacy into a competitive advantage"*[66]. Some describe themselves as *"advocates of data privacy"*[67] and even include promises such as *"offers you affiliated apps to live a better life and puts you in charge of your own data*".[68] These clearly demonstrate the focus on Privacy-as-a-Service and create a reasonable expectation of absolute security on the side of the consumer, which is why the security of these platforms is of utmost importance.

2. Basic Elements

Art. 32(1)(b) GDPR sets out four basic elements of processing systems and services: confidentiality, integrity, availability, and resilience, all of which need to be ensured. These components have actually been well known within the field of information security for a long time and are even considered the cornerstones of operational success, as well as part of the basics in the training of an information security professional.[69] It is therefore advisable to look at already existing standards within information security, which are often very extensive and detailed. This is especially the case since when looking for concrete technical measures and implementation techniques,

---

[64]Cozy Cloud, https://cozy.io/en/ (accessed: 13 April 2026).

[65]Advanced Data Protection Control, https://www.dataprotectioncontrol.org/ (accessed: 13 April 2026).

[66]User Centrics, https://usercentrics.com/ (accessed: 13 April 2026).

[67]Meeco, https://www.meeco.me/ (accessed: 13 April 2026).

[68]My Data Can, https://mydatacan.org/ (accessed: 13 April 2026).

[69]Ustaran / *Room,* Chapter 13, 145; *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 38.

data privacy professionals are often faced with a lack of resources as the GDPR only provides very general guidelines and no comprehensive catalogue of actual, practical methods.[70]

A prime example of a good resource stemming from the field of information security is the ISO/IEC 27000-series, published jointly by the International Organization for Standardization and the International Electrotechnical Commission, which provides best practice recommendations on the security, privacy, and confidentiality of information, as well as IT-governance.[71] Another source could also be the Compendium on IT-Baseline Protection (IT-Grundschuz Kompendium) published by the German Federal Office for Information Security (Bundesamt für Sicherheit und Informationstechnik).[72] Although there is a clear difference between data protection and information security, with the first concerning itself primarily with the protection of the natural person, whereas the latter is focused solely on the assurance of security, availability, confidentiality, and integrity of data in general,[73] there are also many ideas and notions common to both fields. As long as the differences are kept in mind, there seems to be no reason why those two areas should not benefit from each other.

---

[70]In Germany the Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany (Datenschutzkonferenz) published the 'Standard Data Protection Model' (Standard Datenschutzmodell), which is however still being tested regarding its practical usability. See: *DSK*, Standard-Datenschutzmodell.

[71]More information, as well as a list of all the standards within the series can be found under the following link: https://www.iso.org/isoiec-27001-information-security.html (accessed: 13 April 2026).

[72]BSI, IT-Grundschutz-Kompendium.

[73]While those aims are very similar to those referenced in Art. 5(1) and 32 GDPR there are very relevant differences, mainly when it comes to the question of data minimisation. The focus on the individual present in data protection law, explicitly asks for deletion of data, as soon as its processing in no longer necessary. In the field of information security on the other hand, there is more of a tendency to keep data “just in case”, since additional back-ups and/or copies help with achieving the goals of availability and integrity and there is no interest of the individual weighing against such prolonged storage.

a) Confidentiality

Confidentiality refers to the protection of information against unauthorised disclosure.[74] A classic measure against the unlawful retrieval of information is the strict control and monitoring of admission-, entry- and access rights, as well as transfer options.[75] This can, for example, be achieved through implementing a strict authorisation and role concept, the monitoring of the use of authorised resources, or even the separation of certain environments both physical (buildings, rooms) and technical (servers, systems).[76]

Another standard procedure is usually the assurance of secure identification, which should ideally be achieved through the use of multiple factors.[77] Multi-factor authentication requires the existence of two different mechanisms for the assurance of the identity of an individual. Typical mechanisms include passwords, devices, location, or even biometrics.[78] The question of secure identification will actually be important on multiple levels for the security of Personal Information Management Systems. First, the access of the provider and/or its employees to the data (to the extent necessary, if so) will need to be administered. Second, the availability of the data to other parties, in accordance with the preferences set up by the data subject, needs to be assured (this will be of particular importance in the case of consent management tools). Third and most importantly, secure authentication of the data subject itself into the platform needs to be facilitated. Luckily in that area, potential providers of Personal Information Management Services can actually, to a large extent, benefit from existing advancements made by researchers within the

---

[74] *BSI*, IT-Grundschutz-Kompendium, 9.; Sydow/Marsch / *Manz*, Art. 32, para 15.

[75] Paal/Pauly / *Martini*, Art. 32 DSGVO, para 35d; *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 39.

[76] *DSK*, Standard-Datenschutzmodell, 32.

[77] *DSK*, Standard-Datenschutzmodell, 32; *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 39.

[78] Breaux / *Clifton*, 'Identity and Anonymity', 149, 154-158.

area of identification, authentication, and authorisation architectures.[79]

Finally, there is the use of encryption and pseudonymisation, which can arguably be considered as the most important means of protecting the confidentiality of personal data. So important in fact that, while the GDPR tends to be very vague and these two are specifically endorsed in multiple sections, such as Articles 6(4)(e), 32(1)(a), 43(3)(a), as well as Recitals 75, 78 and 83. In consideration of their notability, they should therefore be discussed separately in detail subsequently in this thesis (see: Chapter 2. A. III. 3. Pseudonymisation and Encryption).

b) Integrity

Data integrity concerns the assurance of consistency and correctness of datasets, and deals mainly with questions of protection against data corruption and unwanted manipulation.[80] Typical risk factors are corrupted hardware, software malfunctions, malicious intrusions, or user errors.[81] These risks can be minimised though implementing various measures. Simple errors or bugs within the hard or software can most likely be mitigated though the use of regular patch-management.[82] A much higher risk will result from the potential use of malware, a malicious program designed specifically in order to violate the integrity of the data.[83] Correspondingly to the higher risk there are, however, also numerous controls developed to protect systems from viruses, trojans, ransomware, spyware, keyloggers, and the many other harmful attack schemes out on the market. These include anti-viral software, firewalls, regular system updates,

---

[79] *EDPS*, Opinion 9/2016, para 37.

[80] *Lee/Pipino/Strong/Wang*, 15 JDM 2004, 87, 89 *Zhou/Fu/Yu/Su/Kuang*, 122 JNCA 2018, 1, 1; Borges/Meents / *Cahsor/Sorge*, '§ 10 Datensicherheit, para 3; Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 24.

[81] *Sivathanu/Wright/Zadok*, in StorageSS '05, 26, 27.

[82] Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 24.

[83] Breaux / *Bauer*, 'Cybersecurity and Privacy', 372, 377.

e-mail filtering and penetration testing, as well as network monitoring and logging activities.[84]

Another classic measure used for protecting the integrity of personal data is the use of access restrictions.[85] While these are also effective in supporting other aspects of data security such as confidentiality and resilience, in this case access restrictions serve the function of preventing the tampering of unauthorised individuals with certain datasets, regardless of whether such an individual might act maliciously or is simply making a mistake. One of the must-haves of any system is an access-control mechanism and policy that differentiates between different types of access permissions that users might have, such as read only access, read and write access, or on-demand access (which might, for example, have to be approved by a supervisor or other party).[86] A further useful device for the prevention of such interferences is the use of electronic signatures working with asymmetric encryption, as those guarantee that documents cannot be altered after they have been sealed.[87]

In the context of potential user errors it should, however, be mentioned that these are typically more of a concern in corporate settings where multiple users are working within one environment. When setting up a framework for the functioning of Personal Information Management Systems, the real focus should be a strong authentication mechanism for the user, whereas the provider or other parties would anyway most likely not be granted the rights to make any adjustments to the data subjects' personal data. Also at least worthy of a mention is the option of logging activities, thereby creating audit

---

[84]Paal/Pauly / *Martini*, Art. 32 DSGVO, para 36a; Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 24.

[85]Borges/Meents / *Cahsor/Sorge*, '§ 10 Datensicherheit, para 11.

[86]Breaux / *Bauer*, 'Cybersecurity and Privacy', 372, 382.

[87]*Hagemeier*, 43 DuD 2019, 631, 631; Paal/Pauly / *Martini*, Art. 32 DSGVO, para 36b.

trails.[88] This not only has the potential to mitigate problems of integrity but many other risks mentioned above as well. Most importantly, it will also assure the compliance with the principle of accountability, outlined in Art. 5(2) GDPR.

c) Availability

Availability concerns the assurance that data can be accessed by users and business in accordance with their needs.[89] This feature, however, should not be misunderstood as the requirement to make sure data is constantly accessible to everyone.[90] It should solely focus on guaranteeing that personal data is available for use to the data subject (or entities approved by such) to the extent where this is necessary, as unlimited availability would clearly conflict with most of the general principles of data protection such as confidentiality, data minimisation, or purpose limitation.[91]

Interferences with the data's availability can take multiple forms ranging from delayed access, through to denial of services, up to complete and irreversible destruction of data.[92] The reasons for these issues can typically be traced back to errors in hard or software, malicious attacks, or even simple natural events or disasters such as power outages and disruptions in network connectivity.[93] In that sense, many of the above mentioned security measures will also act as controls for the assurance of availability.

---

[88] *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 40; Paal/Pauly / *Martini*, Art. 32 DSGVO, para 37.

[89] *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 41; Breaux / *Shapiro/Breaux*, Engineering and Privacy', 20, 75.

[90] Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 24.

[91] Breaux / *Shapiro/Breaux*, Engineering and Privacy', 20, 75; *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 41.

[92] Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 25.

[93] Sydow/Marsch / *Manz*, Art. 32, para 16; Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 25.

The primary measure for the assurance of availability is, however, the use of back-ups.[94] This means that multiple replications of a dataset will exist across the system, which might include on- or off-site backup and storage.[95] While definitely in conflict with the principles of data minimisation and storage limitation, this technique is by far the most effective in assuring that data is not lost, taken, changed, or completely deleted where this is not the desired outcome, whatever the potential source of interference might be. This is not to say that data backups can just be created randomly and without limitations, solely based on their effectiveness. In point of fact, as is the case with most fundamental rights and freedoms, the various interests will need to be weighed against each other in consideration of the concrete circumstances in order to find a middle ground accounting for all the rights and interests of the data subject.[96] When balancing these goods against each other, one needs to consider the criticality of the data, meaning how important the data actually is to the individual, the effects of the loss, or even just temporal unavailability might have on the data subject, as well as the intervals in which the information might change. Other, less intrusive measures should be considered if they might achieve the same or at least a similar effect. For example, with protections against power outages or potential disruptions in network connectivity, the existence of an emergency supply source would definitely be equally effective but not require the multiplication of data.[97]

d) Resilience

Last but not least, there is the question of the dataset's resilience. Resilience refers to the ability of a system to continue its operation

---

[94]Paal/Pauly / *Martini*, Art. 32 DSGVO, para 38a; Breaux / *Shapiro/Breaux*, Engineering and Privacy', 20, 75.

[95]Breaux / *Shapiro/Breaux*, Engineering and Privacy', 20, 75.

[96]*Gerling*, 4 RDV 2015, 167, 167; Sydow/Marsch / *Manz*, Art. 32, para 16.

[97]Sydow/Marsch / *Manz*, Art. 32, para 16; *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 41; Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 25.

in spite of adverse conditions and maintain an adequate service level.[98] The scope of what falls under such adverse conditions, however, is very broad and includes such elements as the ability to fend off attacks and large-scale disasters and endure disturbances, as well as a tolerance for high traffic load.[99]

The level of resilience required from a particular operation largely depends on its type, as well as criticality for the user.[100] As we have already mentioned and as will be shown within this thesis, Personal Information Management Systems offer a very large array of services ranging from very basic elements such as pure, secure storage, through to consent management, and even potentially whole "data cockpits" which give the data subject the option to manage the entirety of their personal data within one system. The type of data handled by these PIMS can also differ widely covering work related documentation, data from one's personal and family life, or even information about the individual's health. Based on this, it is virtually impossible to determine a uniform level of resilience required for Personal Information Management Systems. On the contrary, each business model would need to be evaluated separately based on the type of data they process, what purposes they serve, and what the potential impact of service denial or a temporary lack of access for the data subject might be. For example, while the inability to access a tool which simply summarises one's dataflows or puts privacy notices into a standard format in order to make them more understandable, might constitute an inconvenience, it is unlikely to cause any long-lasting harm or damage. If on the other hand, an individual or their doctor could not connect to an electronic patient file, depending on the urgency of the situation the consequences might be severe or even life-threatening.

---

[98] *Mantelero/Vaciago*, in: Software Services, 97, 105; *Sterbenz/Hutchison/Çetinkaya/Jabbar/ Rohrer/Schöller/Smith*, 54 Comput. Netw. 2010, 1245, 1246.

[99] *Sterbenz/Hutchison/Çetinkaya/Jabbar/ Rohrer/Schöller/Smith*, 54 Comput. Netw. 2010, 1245, 1247ff; Gola/Heckmann / *Piltz*, Art. 32 DSGVO, para 31; Paal/Pauly / *Martini*, Art. 32 DSGVO, para 39.

[100] Paal/Pauly / *Martini*, Art. 32 DSGVO, para 39.

While the amount and level of measures implemented for the assurance of a system's resilience will therefore depend on its specific offerings, there are certain standard controls which should definitely be taken into consideration during the set up of a Personal Information Management System. First, the amount of possible points of attack should be reduced as much as possible through the adoption of general security measures that result in a hardening of the systems such as regular updates, patching, firewalls, and encryption.[101] Also, the potential effect of regular employee trainings, cyber security events, or even awareness campaigns with elements such as sending fake-phising messages should not be underestimated in assuring early-on detection, as well as prevention of attacks.[102] The general decentralisation of services in combination with network segmentation has also proven to be quite effective.[103] Last but not least, it should be clear that appropriate business continuity and disaster recovery plans need to be put in place when deploying a Personal Information Management System, regardless of the actual functionalities and criticality of the data.[104] It is furthermore imperative that the creation of these plans takes place in the early stages of implementing such a system, in accordance with the principle of data protection by design and default.

3. Pseudonymisation and Encryption

As already mentioned under Part 1 Chapter 2: A. III. 2. a) Confidentiality, both encryption and pseudonymisation are standard security measures used for the protection of personal data. They are, however, discussed separately as the GDPR seems to endorse those two measures in particular by specifically mentioning them on

---

[101] *Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 32, para 45; Paal/Pauly / *Martini*, Art. 32 DSGVO, para 39.

[102] *CERT-EU/ENISA*, Cyber Resilience, 3f.

[103] Paal/Pauly / *Martini*, Art. 32 DSGVO, para 39; *CERT-EU/ENISA*, Cyber Resilience, 3.

[104] *Mantelero/Vaciago*, in: Software Services, 97, 105.

multiple occasions. This general support is also visible within Art. 32, which specifically singles them out in Paragraph 1 Point a).

a) Pseudonymisation

In accordance with Art. 4 No. 5 of the GDPR, pseudonymisation *"means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*". The removal of certain identifying characteristics often raises the question of whether or not the dataset in question still qualifies as personal data, or whether it should be considered as anonymised since an individual could not be identified from it. Recital 26 resolves that issue by clearly differentiating between the concept of pseudonymisation and anonymisation, also clarifying that pseudonymous data is still to be considered as relating to an identifiable natural person. The differentiation between those two concepts will also be discussed more in depth in the context of defining the extent of the term "personal data" under Part 2 Chapter 3: A. II. 4. c) bb) (2) Anonymisation and (3) Pseudonymisation.

The most basic form of pseudonymisation is the assignment of a "pseudonym" such as a number to individuals and keeping the information connecting the identity of such separately.[105] This can be accomplished through various technical means. Examples include the substitution of identifiers with a number selected by a monotonic counter, the selection of unpredictable numbers by a random number

---

[105] *Voigt/von dem Bussche*, GDPR, 16; Paal/Pauly / *Martini*, Art. 32 DSGVO, para 33; *Schleipfer*, 6 ZD 2020, 284, 285; *Jensen/Lauradoux/Limniotis*, Pseudonymisation techniques and best practices, 21f.

generator, or the use of cryptographic hash functions which take arbitrary input strings and map them to fixed length outputs.[106] It should, however, be considered that the definition of pseudonymisation does not ask for the assignment of a pseudonym. In some instances simply removing certain data-points from a set of information will be more than sufficient, or even potentially more effective than replacing the name or other direct identifier. For example, if we considered a combination of first name, last name, street name and number, postcode and age, the removal of the last name and postcode will most likely be more effective in concealing someone's identity then the first and last name, as the combination of an exact address and age will in most instances make identification quite easy. It should therefore be considered which information a recipient actually requires, as well as to what extent identification based on that data alone would still be achievable.

In Personal Information Management Systems, there are basically two spheres in which pseudonymisation will become relevant. First, it needs to be determined to what extent the provider of the system itself should be given access to data and second, where consent management is part of the provided service offering, the question occurs what kind of data should be transferred to these recipients and how strongly it could or should be pseudonymised. While it is clear that data will always be processed in accordance with the explicit consent given by the data subject, there are many instances in which the actual identity of the individual will be completely irrelevant for the receiving entity and pseudonymous datasets might be more than sufficient for the achievement of their purposes. This is, for example, largely the case in fields such as scientific research, the generation of statistics, or the planning of marketing campaigns.[107] It should thereby be reflected by the technical framework, enabling the

---

[106] *Jensen/Lauradoux/Limniotis*, Pseudonymisation techniques and best practices, 21f.

[107] *Schwartmann/Weiß (eds.)*, Whitepaper zur Pseudonymisierung, 31-37; *EDPB,* clarifications on health research*,* 43-51.

data subject to only disclose data to the extent this is actually necessary for the purpose, in accordance with the principle of data protection by design and default.

The second question relevant for the deployment of a Personal Information Management System, is which of the parties should be performing the pseudonymisation and where the "additional information" through which the data subject could be identified, should be stored. For the most basic models, having secure storage as their main or only service offering, this will be pretty straightforward. With local storage, no processing activities should take place on the side of the service provider. For cloud storage, the security of the data could be ensured via encryption, whereas access by the service provider should either be completely prohibited or limited to strictly technically necessary circumstances. This is also reflected in the current market realities, where most providers have set up their data stores as "zero knowledge" services, meaning that the PIMS provider has no means to access the user's data without the data subjects' explicit consent.[108]

There might, however, be instances where the provider of the PIMS does have an interest in accessing and even further processing the personal data of their customers. This will particularly be the case where the entity's business model is based on providing free services while, for example, analysing the data at hand in order to achieve a profit.[109] Such business models, based on the monetisation of the customers' data while offering seemingly free services, are extremely popular in the current interconnected data economy and it would therefore not be surprising if they were to be transferred to the realm of Personal Information Management Systems.[110] There

---

[108]European Commission, *An emerging offer of "personal information management services" - Current state of service offers and challenges* (23 November 2016) 11.

[109]*Hacker*, 2 ZfPW 2019 148, 148ff.

[110]*Hacker*, Datenprivatrecht, 53; *Elvy*, 117 Columbia Law Rev. 1369, 1384-1386; *OECD*, The App Economy, 25.

are, however, several ethical concerns relating to such schemes,[111] especially from the standpoint of the protection of the individual's rights and freedoms, which is why they should be analysed with much caution and their position as a privacy enhancing technology is highly questionable. The potential use of the customers' data by the PIMS provider can, however, not be categorically excluded from the start and should, therefore, at least be considered as a possibility. In those instances, however, pseudonymisation through a neutral third party acting as a sort of "data custodian" or a "data intermediary" might be advisable in order to assure a high level of protection for the data subjects' rights.[112] Alternatively, pseudonymisation though the data subject could be considered, although this would most likely only work for local-storage models, as otherwise the raw data would in any case be stored and thereby processed by the provider.[113]

Another model more in line with the idea of privacy enhancing technologies and therefore certainly more promising, concerns pseudonymisation in the context of data transfers to other parties, for example, as part of a consent management platform. In this scenario, the PIMS would be acting as a data intermediary in two capacities. On one hand, it would assure that all necessary information has been provided to the individual and based on the freely given, informed, specific and unambiguous consent, then allow the access to that

---

[111] Letter to the EDPB: 'Pay or okay' – the end of a 'genuine and free choice', https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf, 16 February 2024 (accessed: 16 October 2024); https://www.salinger-privacy.com.au/2020/09/28/paying-for-privacy/ (accessed 07 March 2026); noyb, 'Meta (Facebook / Instagram) to move to a "Pay for your Rights" approach', https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach, 3 October 2023 (accessed 16 October 2024).

[112] *Wernick,* 2 TechReg 2020, 65, 70; https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[113] *Jensen/Lauradoux/Limniotis*, Pseudonymisation techniques and best practices, 15.

data to other recipients.[114] On the other hand, the PIMS would, to the extent where this is possible and practicable, pseudonymise the data thereby eliminating the possibility of direct identifiability by the recipient, adding an extra layer of security and as a result, further supporting the principles of purpose limitation and data minimisation, as well as security and confidentiality. It should therefore definitely be considered a significant addition to any business model acting as an intermediary between the potential recipient and the data subject.

b) Encryption

Last, but not least, there is the possibility of encryption, which is probably the central technology used for the protection of data today. Encryption is a method of converting data from an easily interpretable and understandable format (clear text), into a cypher or code which will not be understandable for unauthorised recipients (ciphertext).[115] While some draw a clear line between encryption and pseudonymisation based on the fact that an encrypted dataset still contains all the directly identifying characteristics,[116] others seem to qualify encryption as a type of pseudonymisation technique.[117] Although the question of the technical classification is not really relevant in terms of the outcome, regarding the requirements of the GDPR there is a certain logic in seeing encryption as a (large and quite advanced) subtype of pseudonymisation. While it is true that the unencrypted dataset would contain all the identifying data, this precisely does not apply for the ciphertext, as one would need the decryption code in order to access the information and thereby identify the data

---

[114]For more details on consent management as a function please refer to Part 1 Chapter 2: C. Consent.

[115]Breaux / *Garfinkel*, 'Encryption and Related Technologies', 98, 99; Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 19.

[116]Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 35.

[117]*Art. 29 WP*, Opinion 05/2014, 20f; *Jensen/Lauradoux/Limniotis*, Pseudonymisation techniques and best practices, 22f.

subject. This decryption code can therefore be considered the "additional information", which is kept separately, in accordance with Art. 4 No. 5 GDPR.

When analysing encryption methods, there are fundamentally two types which can be distinguished: symmetric and asymmetric encryption. Symmetric encryption, also referred to as secret-key or single-key encryption, actually dates back as early as 2000 B.C., to the use of "non-standard" or "secret" hieroglyphics and functions by using the same key for the encryption and the decryption of data.[118] This type of encryption relies on the fact that both parties, attempting to communicate without others being able to figure out the content, share a key. This key is used by the first party to encrypt the message, which will then be transmitted via ciphertext to the second party (the recipient) and decrypted through the same key, in order to recover the original message.[119] While most certainly effective in ensuring secure communication, symmetric encryption presents several drawbacks. First, a secure channel needs to be established between the parties for the transmission of the key.[120] Second, in order for this system to function on a large scale, an enormous number of keys needs to be generated and transported regularly.[121] Third, because both parties possess the same key, they will automatically have equal capabilities, meaning that there is also no control against one of them tampering with the information.[122]

Asymmetric, or public-key encryption, is a much more recent technology. It was first introduced in 1976 by cryptographers Whitfield Diffie, Martin Hellman, and Ralph Merkle as a solution to issues identified with symmetric encryption.[123] It operates through the use of two

---

[118] *Paar/Pelzl*, Understanding Cryptography, 2f; Breaux / *Garfinkel*, 'Encryption and Related Technologies', 98, 112.

[119] *Katz/Lindell*, Introduction to Modern Cryptography, 4; *Paar/Pelzl*, Understanding Cryptography, 3.

[120] *Paar/Pelzl*, Understanding Cryptography, 151.

[121] *Paar/Pelzl*, Understanding Cryptography, 151.

[122] *Paar/Pelzl*, Understanding Cryptography, 151.

[123] *Diffie/Hellman*, 22 IEEE Trans. Inf. Theory. 1976, 644, 644ff.

keys: a public and a private key, one of which is used for the encryption and the other decryption of the data at hand.[124] The question of which key will be used for which action will largely depend on the circumstances of the transfer, as well as the desired outcome. For example, e-mail encryption schemes will typically use the public key for the encryption of the message and the private key for its decryption, whereas the opposite is true for digital signatures.[125] The primary advantages of asymmetric encryption include the existence of protocols for the establishment of keys, the assurance of non-repudiation and message integrity, as well as the identification of users through challenge-and-respond protocols.[126] On the other hand, asymmetric algorithms tend to be slower than symmetric keys and also potentially easier to break as they are based on numbers with specific mathematical properties, rather than random pieces.[127]

In Personal Information Management Systems, the selection of the appropriate encryption technique will again largely depend on its pursued functionalities. In the case of a purely secure storage service which is thereby mainly concerned with data at rest, the adoption of a symmetric encryption scheme will most likely be the most efficient. With the addition of other functionalities, such as consent management or the execution of data subject's rights including access, deletion and portability on the individual's behalf, this will, however, not be the case, since these actions will also entail the involvement of parties other than just the user and the PIMS,

Here, in consideration of the issues related to the creation and distribution of keys, as well as secure identification and the assurance of data integrity and traceability, the use of a public key system, at least to a certain extent, will become necessary. For Personal Information Management Systems with multiple functionalities, the deployment of a hybrid cryptographic system combining the use of multiple algorithms will therefore be required in order to assure both the

---

[124]Breaux / *Garfinkel*, 'Encryption and Related Technologies', 98, 126.
[125]Breaux / *Garfinkel*, 'Encryption and Related Technologies', 98, 126.
[126]*Paar/Pelzl*, Understanding Cryptography, 154.
[127]Breaux / *Garfinkel*, 'Encryption and Related Technologies', 98, 127.

security and efficiency of the service.[128] The specifics of such a selected method of encryption will also largely be based and dependent on the current state of the art and thereby possibly require regular re-evaluations.[129]

Another critical question relating to encryption, regardless of the type, is the issue of key management, in particular where the encryption/decryption keys are to be stored. These could either be kept locally on the device of the user, by the PIMS provider, or a third party specifically selected for that purpose.[130] While each of these solutions comes with its own, specific set of advantages and disadvantages, the main factor that needs to be considered while selecting one of these options is the location of the data, as ideally those two should be strictly separated.[131] The requirement to physically separate the data from the cryptographic key is an essential control for the assurance of data security in case of a malicious attack, as otherwise a successful attacker would essentially be able to obtain both the data and the means to decrypt it at once. If, for example, the PIMS provider offered secure cloud storage as part of their service offering, the decryption key could be kept on a device owned by the data subject, which would additionally assure a lack of access from the side of the service provider.[132] Alternatively, if there were concerns regarding the security of the individual's device, as for example mobile phones pose a huge risk in that area, the use of a third-party provider for the key management could be considered.

IV. Interim Conclusions: Storage

The question of storage accompanies every processing activity and the deployment of a Personal Information Management System

---

[128] Breaux / *Garfinkel*, 'Encryption and Related Technologies', 98, 138.

[129] Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 21; Sydow/Marsch / *Manz*, Art. 32, para 12.

[130] *EDPS*, Opinion 9/2016, para 38.

[131] *EDPS*, Opinion 9/2016, para 38.

[132] *Brochot and others*, PDS, 22.

is no exception in that regard. Whether stored locally or in the cloud, users will have a reasonable expectation that their data is being secured in accordance with the highest industry standards, especially if we are to look at the promises given by some of the current providers on the market. With cloud storage, the question of the data centre's location, especially in the context of transfers to third countries, will frequently occur. However, while there may be many obstacles, there are also many chances for improvements in the current market realities which can, and to some extent already have been, introduced by providers of PIMS. Security measures assuring the confidentiality, integrity, availability and resilience of personal data are not only a question of storage, but concern each step in the data lifecycle. In addition to other controls, the use of pseudonymisation and encryption, where possible, is probably the most effective and efficient procedure for the protection of the identifiable individual. If deployed correctly, all of these options have the potential to strengthen the data fundamental principles relating to the processing of personal data, as laid down in Article 5 of the GDPR.

B. Information

The second functionality of Personal Information Management Systems, which is part of this analysis, relates to the provision of information, as required by Articles 13 and 14 of the General Data Protection Regulation. Both Articles contain a long list of details which are to be provided to the data subject either where the personal data is collected directly from the individual (Article 13) or where it has been obtained from other sources (Article 14). This requirement stems directly from the principle of transparency as laid down in Article 5(1)(a), which states that personal data should be processed lawfully, fairly and in a transparent manner.

While transparency seems to be a central postulate of data protection, interestingly enough it was not actually included (at least explicitly) in the previous Data Protection Directive. Article 6(1)(a) of

Directive 95/46 only asked for Member States to provide that data was to be processed fairly and lawfully. According to the Commission itself, this explicit inclusion had the purpose of emphasising that *"transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of their personal data, which could serve as a basis for improved information requirements"*.[133] The Commission thereby identifies the availability of transparent information regarding the processing of personal data as the first step in empowering the data subject to act on their rights and take control of the processing activities concerning them.

Due to its crucial impact, the provision of transparent information should therefore also be considered one of the central functionalities of a Personal Information Management System. The following section will thereby provide an overview of (1) the general requirements, set out by the principle of transparency and the right to information enshrined in the GDPR; (2) the current problems faced by individuals, as well as data controllers and processors when it comes to the provision of such transparent information; and (3) the possible solutions offered by Personal Information Management Systems attempting to alleviate the identified issues and thereby strengthen the rights and freedoms of the data subject.

I. General Requirements

While Article 5(1)(a) GDPR does not provide us with any further details as to when information is considered to be processed in a transparent manner, Recital 39 does lay out a few more specifics. It clarifies that it *"should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed*" and that "*any information and communication relating to the processing of those personal data be easily accessible and easy*

---

[133]European Commission, 'COMMISSION STAFF WORKING PAPER Impact Assessment SEC (2012) 73 final' (25 January 2012) 26.

to understand, and that clear and plain language be used". It further goes on to state that data subjects *"should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*

1. Form

Under Article 12, Paragraph 1 of the General Data Protection Regulation, the information regarding the processing of personal data should be provided to the data subject *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language"*.

In order for information to be considered "concise", it should be brief, reduced to the key aspects of the processing activity but yet comprehensive enough so that all relevant facts and circumstances are contained therein.[134] Lengthy, excessive notices containing many technical details should therefore generally be avoided.[135] The data subject should also be able to easily differentiate between the information regarding the processing of personal data and other areas, such as general terms and conditions of service, the companies' structure, or activities.[136] The purpose of this is to avoid confusion of the data subject, either through information overload or by concealing it by spreading bits and pieces over various channels.[137]

The requirement of intelligibility basically asks for the provided information to be understandable and comprehensible. This often raises the question for whom that would need to be the case. While the Article 29 Working Party names the average member of the intended audience as the relevant point of reference,[138] others have

---

[134]Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 12; Sydow/Marsch / *Greve*, Art. 12, para 14.

[135]*Härting*, DS-GVO, 26.

[136]*Art. 29 WP*, Guidelines on transparency, para 8.

[137]*Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, para 521f.

[138]*Art. 29 WP*, Guidelines on transparency, para 9.

taken the view that the bar should be set significantly below the average level of understanding.[139] Taking into account that the right to privacy is considered a universal human right and that the transparency of information provided to the data subject is one of the fundamental principles of the GDPR, the latter opinion should be followed. It is one of the primary responsibilities of the controller to assure, as far as possible and practicable, that each and every individual affected by the processing conducted within its sphere of influence has the possibility to understand how their data is being used and what the potential consequences are. This does not mean that the target group of a specific service or activity is not to be considered. Quite the opposite, controllers are more than encouraged to consider factors such as the age, level of education, background, language preferences and any other specific characteristics of the intended demographic.[140] While considering all of those factors, they should, however, not be allowed to simply opt for the "average" solution if significant differences within the levels of understanding of specific individuals within a group are to be anticipated. In such instances, the intelligibility for the whole group needs to be aimed at and where a common level for the entire target audience cannot be identified, the creation of multiple privacy notices for different demographics needs to be considered.[141] For instances in which the controller might not be certain whether or not the information provided by them is in fact comprehensible, the Article 29 Working Party encourages the use of mechanisms such as user panels, readability testing, as well as formal and informal dialogues with groups representing the industry, the consumer, or even regulatory bodies.[142]

---

[139]Rücker/Kugler, *Schrey*, D. General conditions, para 606; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 13.

[140]Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 13; Sydow/Marsch / *Greve*, Art. 12, para 20.

[141]Kühling/Buchner / *Bäcker*, Art. 12, para 11; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 13; Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 22.

[142]*Art. 29 WP*, Guidelines on transparency, para 9.

The condition of easy accessibility basically means that the data subject should not have any difficulties in finding the information in question.[143] This means that privacy notices should also be clearly marked as such and detectable without any effort, regardless of the distribution channel.[144] It also means that there cannot be any barriers blocking the access to the privacy notice or making such access more difficult.[145]

Last but not least, the language in which a privacy notice is to be drafted needs to be clear and plain. While the GDPR does not seem to ask for "plain language" in the sense of a specific standard,[146] the Article 29 Working Party does ask for best practices for clear writing to be followed.[147] Regardless of the applicability of any particular standards or practices, it should, however, be evident that the information needs to be phrased in a way that is straightforward and easy to comprehend. The use of technical vocabulary should generally be avoided, unless there is a reasonable expectation that the audience might be familiar with it (for example when communicating with professionals from a particular industry or field) and where absolutely necessary, should be explained to the user.[148] The same goes for long, intricate sentences and complex language structures.[149] Language qualifiers, as well as ambivalent or abstract wording, are also

---

[143]*Art. 29 WP*, Guidelines on transparency, para 11; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 14; Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 21.

[144]Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 14.

[145]Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 21 mentions measures such as password protection or paywalls. The same however would apply for physical restrictions, such as for example making a sign to small or too far away to read.

[146]See more on plain language studies in: *Adler*, in: The Oxford Handbook of Language and Law, 67, 67ff.

[147]*Art. 29 WP*, Guidelines on transparency, para 12.

[148]Paal/Pauly / *Paal/Hennemann*, Art. 12 DSGVO, para 33; Wolff/Brink/v. Ungern-Sternberg / *Quaas,* Art. 12 DSGVO, para 19.

[149]*Art. 29 WP*, Guidelines on transparency, para 12; Paal/Pauly / *Paal/Hennemann*, Art. 12 DSGVO, para 33.

considered problematic as they tend to cause confusion or uncertainty on the side of the data subject.[150]

2. Time

The timely provision of information to the data subject is a crucial component of transparency as well as fairness in the meaning of Article 5(1)(a) GDPR, as even the most comprehensive, coherent and easily available privacy notice will be of no use to the individual if provided at an inconvenient time. This is why the GDPR sets out very specifically at what time information is to be given to the data subject. The question as to when information needs to be provided to the data subject depends on the manner in which it has been obtained.

Where personal data is collected directly from the data subject, Article 13(1) sets out that all relevant details of the processing should be made available at the time of collection. This way the data subject would have the possibility to form an understanding of the planned processing activity prior to its commencement, thereby enabling them to act on their data subject rights such as objection or rectification, before any actions are taken by the controller.[151] Correspondingly, Article 13(2) sets out that the controller would also need to inform the affected individuals in advance if further processing for purposes other than those originally communicated was intended. While the provision of information at the time of collection has the primary objective of assuring transparency for the data subject it will, in fact, frequently benefit the controller from a practical perspective. In most instances, the controller would logically be in active communication

---

[150] *Art. 29 WP*, Guidelines on transparency, para 12f. It should also be noted that such wording might also potentially be in conflict with the principle of purpose limitation, if it was used in order to leave open the option for changes regarding the processing activity. Should there be a specific reason for a certain ambivalence within a privacy notice controllers should generally document these in accordance with the principle of accountability.

[151] Kuner and others / *Zanfir-Fortuna*, Art. 15, 449, 449; Case C-201/14 *Smaranda Bara* [2015] ECLI:EU:C:2015:638, para 33.

with the data subject at the time of collection if data is gathered directly from the individual. It therefore makes sense to use that moment for the provision of information, instead of separately facilitating such in advance or afterward.

Whereas Article 13 provides fairly specific guidelines as to when the controller should inform the data subject regarding the intended processing operation, the same cannot be said for instances where the information is being obtained through sources other than the data subject itself, such as third-party data controllers, data brokers, publicly available sources, or other individuals.[152] For such instances, Article 14(3) establishes that information is to be provided *"within a reasonable period after obtaining the personal data, but at least within one month"*. The article goes on to single out two specific situations: firstly, when personal data is to be used for communication with the individual, all information should be given at the time of that communication and secondly, where disclosure to another recipient is envisaged, then at the latest when data is to be first disclosed. Additionally in the same vein as Article 13(2), Article 14(4) also requires the controller to inform the affected individuals in advance if further processing for purposes other than those originally communicated is intended. The determination of the correct point in time to provide information is thereby slightly more difficult for controllers collecting data from other sources, as they are again faced with the vague terminology of what is "reasonable", having to take into account the specific circumstances of the processing, including what the effect might have on the data subject, as well as their potential expectations.[153] Additionally, the principle of accountability requires them to document the reasoning behind such a determination.[154] This duty of documentation should also not be taken lightly as the Art. 29 WP is of the opinion that, based on the principle of fairness,

---

[152]*Art. 29 WP*, Guidelines on transparency, para 26.

[153]*Art. 29 WP*, Guidelines on transparency, para 28; Kuner and others / *Zanfir-Fortuna*, Art. 14, 434, 445.

[154]Ehmann/Selmayr / *Knyrim*, Art. 14, para 11; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 14 DSGVO, para 17.

information should in general be provided *"well in advance of the stipulated time limits"*.[155]

3. Format

Once the controller has determined what information to provide and when, the question of "how" comes to mind. The lawmakers have again opted for a technologically neutral approach, giving substantial leeway in the selection of the right form of communication. In accordance with Article 12(1) information *"shall be provided in writing, or by other means, including, where appropriate, by electronic means"*. Also, where requested by the data subject, it is allowed to disclose the relevant facts orally, as long as the identification of the individual can be assured. This freedom of choice when it comes to the form of communication, however, should not be interpreted as a sign of indifference or low prioritisation. If anything, it stems from the understanding of the multitude of scenarios and circumstances falling under the regulation, making it impossible to administer clear rules. The definition of processing of personal data (see Part 2 Chapter 3: A. II. 3. Processing and 4. Personal Data) simply covers such a broad array of activities (as well as inactivities) over a basically unlimited number of channels ranging from face-to-face communication to strictly online assessments without any direct contact to the individual, that naturally the form of communication needs to be adjusted to those circumstances in order to be effective and thereby able to reach its objective of transparency.

It should, however, be noted that this freedom of choice will be significantly limited by the principle of accountability. Since the controller will not only be required to provide the necessary information but also to demonstrate compliance with that requirement, most will probably opt for a form that is easy to document such as written and electronic statements or alternatively audio and video recordings,

---

[155] *Art. 29 WP*, Guidelines on transparency, para 28.

where feasible.156 Another indirect limitation stems from Article 12. As noted previously under Part 1 Chapter 2: B. I. 1. Form, information should be presented in a concise, transparent, intelligible and easily accessible form. For the purposes of transparency and intelligibility, it will most likely be necessary to assure that the individual has permanent access in order to allow repeated or more in-depth reviews where desired. Also most importantly, the requirement for an "easily accessible" form consequently also means that the information would need to be provided in a format that is readily available to all data subjects, even if that means the publication over multiple communication channels.[157] For instance in the case of video surveillance, even if the first layer notice clearly refers to a digital source such as a QR-code for the second layer, controllers are still required to make the information additionally available non-digitally.[158]

Last but not least, Art. 29 WP underlines the fact that the word "provide" stipulates a provocative element, meaning that it is not sufficient for controllers to simply make the information available but rather that they have an obligation to actively direct the data subject there.[159] This view is also supported in consideration of other language versions[160] and the existing case law,[161] and is regarded the prevailing opinion in literature.[162]

---

[156]Kuner and others / *Polčák*, Art. 12, 398, 408; Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 24.

[157]Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 22; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 14 DSGVO, para 18; Kuner and others / *Polčák*, Art. 12, 398, 408.

[158]*EDPB*, Guidelines 3/2019, para 117.

[159]*Art. 29 WP*, Guidelines on transparency, para 33.

[160]The German wording "übermitteln" can be translated to "transfer"; the French "fournier" to "supply" and the Polish "udzielić" to "give", all of which are verbs requiring an element of action from the respective subject.

[161]Case C-375/15 *BAWAG* [2017] ECLI:EU:C:2017:38, para 48.

[162]*Kahler*, in: Turning Point, 13, 15; Kühling/Buchner / *Bäcker*, Art. 12, para 16; *Kamps/Schneider*, 1 K&R-Beilage 2017, 24, 26; Ehmann/Selmayr / *Knyrim,* Art. 14, para 13.

4. Costs

As per Article 12(5) GDPR, all information concerning the processing should be provided free of charge. While the Article also provides an exemption for “manifestly unfounded” and “excessive” requests in order to protect the controller from individuals abusing their rights solely for the purpose of causing damage, those do not apply to the right to information under Articles 13 and 14 discussed previously.[163] The wording clearly refers to “request”, meaning instances where the enforcement of a right would require a demand from the data subject. As detailed, the complete opposite applies to the right to information as it specifically contains a proactive element on the side of the controller and thereby applies regardless of any activity from the concerned individual.

5. Exemptions

The GDPR does, however, name a number of exceptions under which information does not need to be provided to the data subject, most notably where the individual in question already has the information (Art. 13(4) and 14(5)(a)). Also, where the data is not obtained directly from that person, they also do not need to be informed in case this would prove impossible or would involve a disproportionate effort (Art. 14(5)(b)); where obtaining or disclosure is expressly laid down by Union or Member State law (Art. 14(5)(c)); or where the personal data must remain confidential (Art. 14(5) d)). Although all of these exemptions bear many legal questions with regard to their extent, interpretation, and practical enforceability, these should not be discussed here. While they are most certainly important for the understanding of the right to information as a whole, they are not particularly relevant in the context of Personal Information Management Systems as instances where such an exemption would be applicable would render any PIMS supporting that right unnecessary.

---

[163] Kühling/Buchner / *Bäcker*, Art. 12, para 36; Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 37.

II. Obstacles

What is relevant, however, are the practical problems occurring with the assurance of this right, as those will directly relate to the possible functionalities of a Personal Information Management System. As has already been mentioned, the availability of transparent information with regard to the processing of personal data should be considered the first step in empowering the data subject to act on their rights and take control of the processing activities concerning them. This section will therefore provide an overview of current problems faced by individuals, as well as data controllers and processors when it comes to the provision of such transparent information.

1. Conflict of Objectives

As per Recital 39 of the GDPR *"[t]he principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used*". Solely from this sentence, the strong conflict of objectives extending itself through Articles 12–14 is already evident. On the one hand, as discussed previously, Article 12 of the GDPR requires that all information is to be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Lengthy, excessive notices containing many technical details, are to be avoided. All information should be phrased simply and be easy to comprehend, and the data subject should have no difficulties in accessing it all at once. On the other hand, Articles 13(1) and (2) and 14(1) and (2) contain an extensive list of facts that need to be provided to the affected parties, including not only such basics as the purpose and legal basis of processing, but details such as transfers to third countries, storage periods and data subject rights. As per Recital 39 *"[i]t should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed"*.

This, however, means that the controller, in order to assure complete transparency would need to communicate the entire data lifecycle to the individual. Doing so without a lengthy notice is virtually impossible, since simply covering all of those points, even if each of those would only contain a brief illustration, would result in a multi-page document. Moreover, it needs to be considered that most controllers will have to communicate multiple processing activities which are potentially related and intertwined with each other, adding even more confusion to the matter.[164] Providing truly detailed and comprehensive information will therefore regularly contradict the requirement of intelligibility, as such notices will be hard to understand.[165] Finally, while it is understandable that the lawmakers would want to avoid the use of technical terms in such notices, it is not clear how controllers are to explain certain technical aspects of the processing, especially when it comes to the use of technologically advanced methods of analyses, tracking and targeting, without referring to the proper terminology.[166] The fact that certain processes and mechanisms will simply not be understood by a layperson without providing them with a large amount of background information and additional resources, is unfortunately an unavoidable part of the implementation of innovative technological and organisational solutions. This conflict of objectives whereby controllers are urged to transparently communicate all details of their processing activities towards the data subject but on the other hand are penalised for the creation of lengthy and incomprehensible privacy notices, ultimately leaves even those entities which are highly motivated to comply with all privacy regulations in a constant struggle between meeting the different aims.

---

[164] *Hacker*, Datenprivatrecht, 155; Wybitul / *Pötter/Bausewein*, Art. 15 DSGVO, 310.

[165] *Hermstrüwer*, Selbstgefährdung, 88; *Kamps/Schneider*, 1 K&R-Beilage 2017, 24, 25; *Hacker*, Datenprivatrecht, 155; Kühling/Buchner / *Bäcker*, Art. 12, para 12; *Gluck and others*, SOUPS '16, 321, 322.

[166] *Abiteboul / Stoyanovich*, 11 JDIQ 2019 1, 4; *Blacklaws*, 376 Phil. Trans. R. Soc. A. 2018, 1, 6; *Kamps/Schneider*, 1 K&R-Beilage 2017, 24, 25.

The practical issues arising from the described conflict of objectives are well known in literature[167] and have been explicitly recognised by the Art. 29 Working Party[168]. Taking that into consideration, there are multiple best-practice solutions suggested to controllers in order to consolidate the conflicting requirements. The most commonly used are so called "layered" privacy notices, in which the data subject is given a basic overview of the relevant information in the first "layer", while simultaneously being given directions as to where additional information can be found.[169] The underlying idea is that individuals would not be overwhelmed in the first instance, giving them a general overview regarding the processing activity and also facilitating the possibility of finding out more, where necessary.[170]

While most certainly a reasonable measure in practice, the layered approach can also only remedy the inherent problems with the

---

[167] *Auer-Reinsdorff,* 'Transparente Datenschutzhinweise – den inhärenten Widerspruch auflösen!', 4 ZD 2017, 149, 149ff; Kuner and others / *Polčák*, Art. 12, 398, 407; Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 23; Paal/Pauly / *Paal/Hennemann*, Art. 12 DSGVO, para 28; Kühling/Buchner / *Bäcker*, Art. 12, para 12; *Kamps/Schneider*, 1 K&R-Beilage 2017, 24, 25.

[168] *Art. 29 WP*, Guidelines on transparency, para 34: "*There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible".*

[169] The use of layered privacy notices can be observed on virtually any larger website, either in the form of FAQ, giving additional input, once a particular question is selected. For example: Amazon, https://www.amazon.de/-/en/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (accessed: 15 April 2026); Microsoft, https://privacy.microsoft.com/en-us/privacystatement (accessed: 15 April 2026); Google, https://policies.google.com/privacy?hl=en-US#infosharing (accessed: 15 April 2026); Atlassian, https://www.atlassian.com/legal/privacy-policy#how-we-store-and-secure-information-we-collect) (accessed: 15 April 2026). Also popular are "see more for" buttons, which lead the user to a new page containing more detailed explanations. For example: X, https://x.com/en/privacy (accessed: 15 April 2026); YouTube, https://www.youtube.com/howyoutubeworks/our-commitments/protecting-user-data/ (accessed: 15 April 2026); Meta, https://www.facebook.com/privacy/policy (accessed: 15 April 2026).

[170] *Art. 29 WP*, Guidelines on transparency, para 35.

provision of transparent information to a certain extent. Ultimately layered privacy notices from larger providers with elaborate, interconnected processing activities are still far from concise and often leave the user with an intricate and convoluted web of references, links and buttons, with information found in various locations thereby requiring multiple actions from the user in order to obtain a comprehensive overview.[171] This impression is largely supported by studies in the field showing that layered notices do not seem to improve the understandability and may even leave the individual with incorrect impressions.[172] Aware of this fact, the Art. 29 WP again proposes a number of additional tools to be used in order to improve comprehensibility such as "push"[173] and "pull"[174] notices, icons, QR-codes, voice alerts and videos.[175] In the same vein, many researchers have also taken an interest in the topic and have made further suggestions

---

[171]This problem is for example well evidenced by one of the proceedings issued against Google by the CNIL. Here the Supervisory Authority imposed a fine of 50 million, against the tech-giant, on the basis of multiple violations, including the lack of adherence to the principle of transparency. Googles privacy policy at the time not only included comprehensive information regarding their processing activities, but also made use of the layered approach, as well as many other elements promoted by the Art. 29 WP, such as icons, push and pull notices and even explanatory videos. Still the CNIL considered those as only partially supporting the facilitation of transparency and determined that the relevant information was ultimately excessively scattered and hard to access. See: 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC' para 97, https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf (accessed: 18 April 2026).

[172]*McDonald and others*, in: PET, 37, 53; *Gluck and others*, SOUPS '16, 321, 322; *Karegar/Pettersson/Fischer-Hübner*, 23 ACM Trans. Priv. Secur. 2020, 1, 2.

[173]"Push" notices, also referred to as "just-in-time" notices provide the data subject with information at the exact time of collection, for example in the form of a small pop-up explaining the purpose of collecting certain data points, while doing so via an online form or questionnaire.

[174]"Pull" notices, also referred to as "privacy dashboards" are a single point on the website where the privacy preference of the individual can be managed for a specific service.

[175]*Art. 29 WP*, Guidelines on transparency, para 39f.

for achieving greater comprehensibility and availability of privacy notices. Examples include solutions such as the use of privacy nutrition labels[176], focusing on the communication of unexpected practices,[177] visceral notices,[178] comics,[179] icons,[180] or even personalised notices.[181] To what extent those are, however, actually effective or whether they are rather to be considered as a "nice" addition is still not clear.[182]

Also, regardless of their actual effectiveness, it remains questionable to what extent controllers would be willing to incorporate those into their content, since the creation of such engaging elements requires a substantial amount of resources that many entities might simply not have, or not be willing to invest. Ideas, such as the creation of special design places which *"should be leveraged as part of a comprehensive design process that focuses on audience-specific privacy notice requirements and considers a system's opportunities and constraints in order to develop a notice and choice concept that is well integrated with the respective system*"[183] are certainly innovative and in line with the principle of data protection by design and default but might ultimately not be able reach general recognition due to the substantial effort required from controllers, as well as the potential risks involved in implementing new solutions. A standard hazard that typically comes with innovation is insecurity. When creating

---

[176]*Kelley and others*, in: CHI '10, 1573, 1573ff.

[177]*Gluck and others*, SOUPS '16, 321, 322.

[178]*Calo*, 87 Notre Dame Law Rev. 2013, 1027, 1034-1041.

[179]*Tabassum and others*, in: 2018 CHI Conference, 1ff; *Knijnenburg/Cherry*, SOUPS 2016.

[180]*Efroni and others*, 5 EDPL 2019, 352, 352ff; *Rossi/Palmirani*, in: Big Data Age, 181, 181ff; *Holtz/Zwingelberg/Hansen*, in: Privacy and Identity Management for Life, 279, 279ff; *Holtz/Nocun/Hansen*, 6th IFIP, 338, 338ff; *Geminn/Francis/Herder*, 14 ZD-Aktuell 2021, 05335.

[181]*Harbach and others,* in: CHI '14, 2647, 2647ff.

[182]*Doan and others*, in: WWW '22, 534, 541; *Karegar/Pettersson/Fischer-Hübner*, 23 ACM Trans. Priv. Secur. 2020, 1, 2; *Gluck and others*, SOUPS '16, 321, 322; *McDonald and others*, in: PET, 37, 53.

[183]*Schaub and others*, SOUPS 2015, 12.

company policies, compliance and privacy departments will most likely look at existing practices and analyse how these are being perceived by the authorities. New solutions, however, come with the inevitable downside of not having been tested live and making their operation not entirely predictable. Unpredictability in turn leads to potential liability, ultimately resulting in the fact that departments, who are explicitly tasked with the reduction of risk, are unlikely to advise on implementing such solutions, instead opting for a potentially long and unclear notice but covering all points listed in Articles 13 and 14. Also, since data protection departments are not directly profitable, businesses are often reticent about assigning additional funds toward them. Considering all the requirements the GDPR puts on controllers such as keeping records of all processing activities, training employees, answering data subject requests etc. it is imaginable that the facilitation of the most innovative, advanced and visually appealing privacy notice would not be on top of their priority list, unless they would be explicitly tasked to do so by the DPAs.[184]

2. Lack of Information

Directly linked to this potentially low prioritisation of privacy notices is the far more prosaic problem of incomplete and incorrect privacy notices. Especially in the online environment, privacy policies often fail to disclose legally required information. A review of the policies of eight streaming service providers conducted in 2019 by the nonprofit organisation noyb evidenced that for almost all major providers, information regarding the storage period, third country transfers, recipients and data subject rights were either incomplete or completely missing.[185] A similar conclusion was also reached by a prior study, according to which among the collected notices of retailers, internet

---

[184]As noted in: *Pollach*, '50 Commun. ACM 2007, 103, 107: „The findings noted here suggest that online privacy policies have been drafted with the threat of privacy litigations in mind rather than commitment to fair data handling practices".

[185]*Zimmer*, Streamingplattformen, 9.

service providers, news sites and travel agents, 39.4% of privacy related questions could not be answered based on the policies alone, due to a lack of information.[186] The authors of the noyb report also criticised the frequent use of very general wording[187] and the lacking of a connection between the categories of data, the purpose of their processing, and the legal basis.[188] Both research and practical experience show that the use of vague and unambiguous terms seems to be the rule, rather than the exception in the online environment.[189] Other typical problems also include a lack of readability or trouble accessing policies, with some applications reportedly not having privacy notices at all.[190]

While in some instances the reasons for these shortcomings can definitely be traced back to a purposeful omission or imprecision created to deceive users, often the reasons are far more mundane. In many instances, general wording is simply being used in order to cover as many processing activities as possible. Phrases such as "as long as necessary for the purpose"; "might share/transfer"; "where required" etc. are so broad that they can apply to a wide range of processes, seemingly releasing the controller from the responsibility of writing a separate text for each operation. Many might also hope to simultaneously cover future changes to processing activities or even completely new processes.

This applies in particular to elements of these procedures which are frequently subject to changes, such as sub-processors, recipients, sources or tools used for processing, as re-reviewing and adapting multiple notices across a range of products each time a minor change within the process is being made is a rather cumbersome

---

[186] *Pollach*, '50 Commun. ACM 2007, 103, 105.

[187] For example: data being stored „as long as necessary" or that data „might" be shared with third parties.

[188] *Zimmer*, Streamingplattformen, 10.

[189] *Reidenberg/Bhatia/Breaux/Norton*, 45 J. Leg. Stud. 2016, 163, 163ff; *Pollach*, '50 Commun. ACM 2007, 103, 106f.

[190] *Fowler/Gillard/Morain*, 21 Health Promotion Practice 2020, 679, 681; *O'Loughlin and others*, 15 Internet Interv. 2019, 110, 114; *Sunyaev/Dehling/Taylor/Mandl*, 22 JAMIA 2015, e28, 31.

task and some might argue even superfluous, as it is debatable to what extent data subjects actually care about changes such as the use of a different service provider. These practical issues with the simple management of policies are particularly well evidenced in an analysis conducted on the effectiveness of privacy policies for voice assistant applications. The study identified that a large amount of URL links on Google and Amazon were either broken or inactive.[191] Also, even in policies which showed significant attention to detail, updates made to certain skills were not always properly reflected, suggesting that a lot of effort was put into the initial draft but that providers struggled to always incorporate changes accordingly.[192] This shows that inaccuracies in privacy policies are not necessarily a sign of bad faith or a low level of care on the side of the controller but rather mismanagement. In contrast to such obligations as keeping a record of processing activities, training employees, or executing erasure policies, the creation of a privacy policy is often considered more of a singular exercise (which needs to be completed once, but does not require further action) rather than an ongoing process. Businesses should therefore be advised to build additional controls into their existing processes such as automatically requiring a review of the current policies in cases where changes to the record of processing are being made.

3. Inconsistencies

The final hindrance in the creation of a concise, transparent, intelligible and easily accessible privacy policy which enables the data subject to understand how and why personal data concerning them is being processed, is inconsistency. The inconsistency problem identified here does not refer to differences between the actual processing operation and the information found in the notice, or disparities between multiple notices and policies of one controller. The hin-

---

[191] *Liao and others*, in: ACSAC '20, 856, 860.
[192] *Liao and others*, in: ACSAC '20, 856, 861.

drance presented here refers to the extreme differences in both visual and textual presentations of fact, done by different service providers.

For example, as has been mentioned above earlier under Part 1 Chapter 2: B. II. 1. Conflict of Objectives, the use of layered privacy notices has become one of the most commonly applied tools in dealing with the conflicting requirements of concision and transparency. While these multi-layered notices are to be considered an industry standard, the way the relevant information is structured, presented or even phrased is far from standardised. Amazon uses a visual design similar to a Wikipedia page with the entire text continuously running through the page, but incorporating a general overview of contents at the top, which allows the user to directly jump to a specific section.[193] The Microsoft Privacy Statement also has a similar menu for navigating between sections of the text; it is however located at the left side rather than on top.[194] Additionally each section is equipped with a "learn more" button, which if selected reveals additional information about each point. Google navigates the varying sections via a column on the left as well, but includes a large amount of visuals, including icons and videos, in between sections.[195] X, on the other hand, mixes different forms of the layered notice. It primarily relies on drop-down FAQs within each relevant section but also incorporated boxes with "learn more" buttons on top, which either lead to one of the sections on the page or to a sub-page depending on the content.[196]

Similar disparities can be observed in the used wording. Information regarding data subject rights can be found under headings

---

[193]Amazon Privacy Notice, https://www.amazon.de/-/en/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (accessed 15 October 2025).

[194]Microsoft Privacy Statement, https://privacy.microsoft.com/en-us/privacystatement (accessed 15 October 2025).

[195]Goole Privacy & Terms, https://policies.google.com/privacy?hl=en-US#infosharing (accessed 15 October 2025).

[196]X Privacy Policy, https://x.com/en/privacy#_blank (accessed 15 October 2025).

titled: *"How to access and control your personal data",*[197] *"Exporting & deleting your information"* and *"Your privacy controls",*[198] *"You can control your experience",*[199] or

"What information can I access?" and *"What choices do I have?"*[200]. In the same vein, various synonyms are used for the purposes of processing, such as *"Why Google collects data?"* (Google), *"How we use personal data"* (Microsoft), *"For what purposes does Amazon Europe process your personal information?"* (Amazon) or even *"Learn how we make your data work"* (X). Adding to that diffusion is the fact that all of these points are organised in a different order in each policy, with some requirements of Articles 13 and 14 GDPR summarised under one position or multiple ones, depending on the choice of the controller. This is not to say that any of these choices are wrong or misleading; it instead evidences how these differences in stylistic choices lead to inconsistencies in the visual and linguistic presentation of the facts. It should also be noted that these are just a few examples (selected due to the high outreach of these controllers) out of a countless number of privacy policies found online, which also means that data subjects are potentially confronted with an immeasurable number of variations.

As discussed under Part 1 Chapter 2: II. I. 3. Format, this diversity is admittedly completely in line with the recommendations of the Art. 29 WP, as well as the prevailing literature, which to a large extent grants the controllers freedom of format in order to allow adaptation of the notice to the circumstances of each processing activity. The potential risk resulting from these discrepancies, however, lies in the

---

[197]Microsoft Privacy Statement, https://privacy.microsoft.com/en-us/privacystatement (accessed 15 October 2025).

[198]Goole Privacy & Terms, https://policies.google.com/privacy?hl=en-US#infosharing (accessed 15 October 2025).

[199]X Privacy Policy, https://x.com/en/privacy#_blank (accessed 15 October 2025).

[200]Amazon Privacy Notice, https://www.amazon.de/-/en/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (accessed 15 October 2025).

fact that individuals who are not well versed with the aspects, vocabulary and regulations applicable in the field of data protection might have trouble finding and understanding the elements which are of interest to them. Humans are, after all, creatures of habit and individuals might be more capable of comprehending certain facts if they include recognisable elements. This idea was indirectly supported in a study, which compared the effectiveness of different types of interactions engaging users with consent forms. [201] A laboratory experiment was conducted on 80 individuals in four different groups in two phases.[202] The results showed that initial differences between the presented types of user engagement observed in Phase 1 virtually disappeared in Phase 2 after the users were repeatedly exposed to the consent forms and that the participants became equally successful at noticing the crucial elements of the policies, as well as remembering what type of processing for which they had provided their consent.[203] Based on that, the researchers concluded controllers should opt for the same type of user engagement for the entirety of the policy in order to avoid biases in user attention.[204] While these recommendations apply to engagement types within a consent form, the general conclusion that familiarity would in principle result in better understanding and that a consistent form of presentation would likely reduce biases, can be applied to privacy policies in general as well.

While the idea of inconsistencies between varying policies as a hindrance to transparency does not seem to be widely analysed in the prevailing literature in the field, it is in fact discussed in the context of privacy icons with researchers supporting the idea of promoting one standardised icon set in order to increase their efficiency and usability.[205] The idea of using ideas and patterns recognisable to the

---

[201] *Karegar/Pettersson/Fischer-Hübner*, 23 ACM Trans. Priv. Secur. 2020, 1, 1ff.

[202] ibid 11f.

[203] ibid 34f.

[204] ibid 35.

[205] *Efroni and others*, 5 EDPL 2019, 352, 366 *Holtz/Nocun/Hansen*, 6th IFIP, 338, 346; *Rossi/Palmiran*, 36 Design Issues 2020, 82, 95f.

user has been examined in the context of visceral notices as well, with the author concluding that *"familiarity breeds a kind of opportunity"*.[206] This opportunity might be utilised in two main aspects, the first being the already discussed enhancement of understandability due to the incorporation of instantly recognisable patterns. The second aspect pertains to the possibility of simplifying the comparison between policies. Due to the current discrepancies in the visual and linguistic presentation of the facts, it is significantly harder for data subjects to accurately ascertain the differences in which various service providers handle their personal data without conducting an in-depth analysis of each policy first. It is thereby virtually impossible for users to accurately weigh all advantages and disadvantages of a product against each other, since they would first need to invest a substantial amount of time into simply locating the relevant information. If, on the other hand, privacy policies used a standardised format, comparing and contrasting practices of the particular controllers would be significantly easier.

III. Proporals for Improvement

As demonstrated above, both controllers and data subjects experience significant hurdles in respectively providing and receiving transparent information regarding the processing of personal data. The ability to understand and assess how this data is being handled is, however, the first and thereby most essential step in empowering users to gain control over their data. This is why the provision of transparent information should be considered one of the central functionalities of a Personal Information Management System. The following section will therefore analyse how PIMS might alleviate some of the discussed challenges, thereby strengthening the rights and freedoms of the individual.

While there is a large number of tools currently being offered and developed on the market which to a degree vary, for the purpose of

---

[206] *Calo*, 87 Notre Dame Law Rev. 2013, 1027, 1035-1038.

this thesis when it comes to the specifics of their design and set-up they will be broadly divided into a) interpretative; b) auditing; and c) responsive tools. It should be noted that this classification is not based on any official designation. While there have been varying attempts at categorising transparency enhancing technologies,[207] the here presented framework explicitly serves the purpose of facilitating their analysis in the context of the roles and responsibilities of these Personal Information Management Systems vis-à-vis the data subject. Certain functionalities which might typically be offered collectively under the current market realities, would still require a separate analysis for the purpose of this thesis.[208] The provided overview of the existing offerings serves that same objective and is neither to be considered exhaustive nor final. The selected examples are simply

---

[207]For example: *Hedbom*, IFIP 2009, 67, 67ff, introduces a classification based on: possibilities of control and verification, target audience, scope, trust requirements, information presented and other aspects; *Janic/Wijbenga/Veugen*, in: STAST 2013, 18, 24, categorized tools based on what type of insight into the data lifecycle they were providing (intended collection, stored data, disclosures to thirds parties etc.); *Hansen*, in: Future of Identity, 199, 209-216, outlines four main areas of related transparency tools: information on interaction partners, understanding privacy policies, exercising privacy rights online, and a news feed on security and privacy incidents; *Zimmermann*, Amsterdam Privacy Conference, uses a long list of criteria to construct a grouping into the following categories of TET: Assertion, Awareness, Declaration, Audit, Intervention and Remediation.

[208]For example: as mentioned under Part 1 Chapter 2: A. Storage this functionality will in most instances be accompanied by other offerings such as data sharing, organisation and password management. The same can to an extent also be said about tools attempting the assurance of transparency. The term transparency enhancing technologies in usually used in a much broader sense, not only covering services aimed at the assurance of the right to be informed as outlined in Articles 13 and 14 GDPR, but also other data subjects rights (access, erasure, portability etc.) considering them all part of assuring that the consumer is not only formally informed, but also aware and involved in the processing of personal data (see for example: *Hedbom*, IFIP 2009, 67, 69; *Janic/Wijbenga/Veugen*, in: STAST 2013, 18, 18; *Hansen*, in: Future of Identity, 199, 205. In the context of analysing the role the PIMS takes towards to data subject it is however necessary to view these functionalities separately at first.

used in order to illustrate general tendencies, considerations and developments.

1. Interpretative

Broadly speaking, interpretative tools serve the purpose of extracting the information relevant to each user from privacy policies and presenting it in a coherent and intelligible way, thereby in a sense providing an interpretation of the available text by translating it into a more comprehensible format. Since providing manual transcriptions is virtually impossible, these tools usually rely on a combination of natural language processing and either supervised or unsupervised machine learning. [209]

a) Polisis

Polisis, for example, is an online service which once given an URL, scrapes the policy of the web page and then divides and combines the privacy relevant information into segments.[210] Should the produced segments be too long, they are further subdivided into a hierarchy of classifiers, with the top level defining high-level privacy categories and the lower levels describing a set of privacy attributes, each assuming a set of values.[211] Once the data is structured and classified, Polisis uses Disconnect[212] privacy icons and colour assignments to provide a high-level overview and rating of the provider's privacy practices, presented within the policy.[213] The application also visualises the produced results by presenting the data flow and its logic, as well as the choices given to the user in the privacy policy.[214] According to the authors, Polisis can achieve an accuracy

---

[209] *Hacker*, Datenprivatrecht, 567; *Pałka/Lippi*, in: Big Data Law, 115, 115ff.
[210] *Harkous and others*, USENIX 2018, 531, 533-535.
[211] ibid 534f.
[212] Disconnect, https://disconnect.me (accessed 15 October 2025).
[213] *Harkous and others*, USENIX 2018, 531, 537f.
[214] ibid 544.

of 88.4% in the provision of such automatically translated privacy notices.[215] Based on the same methodology, they have subsequently also introduced PoliCompare which focuses on the comparison of data processing practices of multiple providers.[216] It allows users to select a maximum of ten providers whose privacy policies are analysed by the application and then displayed in the form of a table, contrasting their guidelines against each other, as well as underlining positive and unfavourable aspects of each.[217] In consideration of this part of the service, the question does come to mind what the consequences of choices made by the data subject, based on inaccurate results, might be. After all, Polisis does not provide an overview of the actual processing activities of the service providers it questions, but rather those which have been declared, leaving vast room for inaccuracies both as a result of incomplete notices, as well as mistakes made by the underlying algorithm. In the end, however, those risks would probably not be higher than if the individual reviewed each policy on their own, as omissions and oversights would likely be encountered there as well.

b) The Usable Privacy Project

Another large initiative working on the development of a scalable technology, which could semi-automatically translate and present the content of a website's privacy policy into an easily comprehensible format for users, is the Usable Privacy Project.[218] The project is working on the development of algorithms that would facilitate the interpretation of such privacy notices in consideration of identified user concerns.[219] For that purpose, the algorithms operate across

---

[215]ibid 532.

[216]PoliCompare, https://www.epfl.ch/labs/lsir/policompare/ (accessed 15 October 2025).

[217]PoliCompare, https://www.epfl.ch/labs/lsir/policompare/ (accessed 15 October 2025).

[218]The Usable Privacy Policy Project, https://usableprivacy.org/learn_more (accessed 15 October 2025).

[219]*Sadeh and others*, Usable Privacy Policy Project, 3.

several strands including not only the semi-automated understanding of privacy policies and their analysis but also the modelling of privacy preferences for the determination of relevant disclosures and the mitigation of deleterious cognitive and behavioural biases in such.[220] This interdisciplinary approach results in quite interesting considerations in connection with the assurance of transparency. For example, in the context of privacy preference modelling, the potential differences between the type of information that would need to be displayed or even flagged as critical to the users based on the type of website they are visiting, were explored.[221] The underlying idea is that users might be comfortable with the collection of certain types of data or particular processing activities in one context, but deem it completely inappropriate in another.[222] Incorporating considerations such as these would in turn allow the provider to remove certain irrelevant elements from the policy, thereby enabling the data subject to put more focus on the aspects crucial for them.[223]

The research project also explores questions such as the differences between ex ante and ex post user privacy preferences,[224] as well as cognitive and behavioural biases contemplating the possibilities of nudging users into privacy friendly choices they will not later regret.[225] Problems such as the privacy paradox, availability heuristics, bounded rationality, and status quo bias are well known and have been discussed in the realm of data privacy for some time

---

[220]ibid 3f.

[221]ibid 6.

[222]For example, users might be absolutely comfortable sharing location data, with an app providing whether warnings, advising on public transportation options or recommending nearby restaurants, but would be uncomfortable if the same data was collected by an online game or ebook reader. In the same vain might be more likely to be interested in the encryption techniques used by their Messenger application or online banking application, than their Netflix account.

[223]*Sadeh and others*, 'Towards Usable Privacy Policies, 2.

[224]„Ex ante" referring to the state before the decisions about a specific processing operation is being made (here called „privacy sensitive event") and „ex post" to their perspective after said event.

[225]*Sadeh and others*, Usable Privacy Policy Project, 3.

now.[226] Also, since they are paramount with regard to the discussion on the collection of valid consent, they shall be analysed further in that context subsequently.[227] It should, however, be noted at this point that the addition of these types of considerations has the potential to significantly broaden the scope of the service, beyond solely the "interpretative" element. Simply considering the viewpoint of the data subject and their interests and biases when deciding on how to present the relevant information still lies within the sphere of assuring intelligibility for the intended audience. Once the service includes a more advisory component, whether direct or indirect, which attempts to steer the user into a certain direction, an element of active involvement of the service provider into the decision-making process of the individual emerges and the potential processing activity as a whole starts to appear. While subtle at this point, this signifies a clear shift regarding the extent of influence exerted on the processing of the personal data of the individual. The extent of this influence will thereby have to be carefully considered when assessing the roles and responsibilities of the Personal Information Management System towards the data subject, as well as the data controller, whose policy is being presented.

c) PrivacyGuide

A privacy policy summarisation tool which has been directly inspired by the General Data Protection Regulation is PrivacyGuide.[228] The system also applies machine learning and natural language processing techniques for its functioning and comprises a stand-alone application using Java as the programming language.[229] The eleven GDPR-relevant privacy aspects selected by the researchers are dis-

---

[226] *Soh,* 5 EDPL 2019, 65, 65ff; *Barth/de Jong*, 34 TELEMAT INFORM 2017, 1038, 1038ff; *Deuker*, in: Privacy and Identity Management for Life, 275, 275ff; *Acquisti/Grossklags*, 3 IEEE Security & Privacy 2005, 26, 26ff.

[227] See Part 1 Chapter 2: C. III. Behavioural Obstacles.

[228] *Tesfay and others*, in: IWSPA '18*,* 15, 15ff.

[229] ibid 17.

played in a user interface consisting of a dynamic dashboard, including a summary of each category accompanied by an icon with an appropriate colouring for each risk level.[230] According to the conducted research, the content of the reviewed privacy policies was displayed with an average accuracy of 74%, whereas the risk level assigned to each aspect was even higher, with 90% accuracy.[231]

d) PrivacyCheck

Also concerned with presenting privacy policies in a coherent and intelligible way is PrivacyCheck.[232] This browser add-on was designed to provide a general overview of a company's privacy policy through graphical means.[233] Similar to Polisis, the user needs to provide the URL of the policy they wish to be analysed.[234] The tool, however, is not intended to give in-depth information on the details of each processing activity but in line with the approach taken by the Usable Privacy Project, primarily aims at providing a broad overview. In order to do so, it focuses on ten relevant privacy factors which have been identified as crucial to the data subjects' interests.[235] The data mining classification model then assigns a risk level (green—low, yellow—medium, red—high) to each of these factors.[236] The model was trained by a corpus of 400 randomly selected privacy policies which were manually assigned risk factors.[237] In 2020, the creators of Privacy Check presented the addition of a new component to their service, namely the Competitor Analysis Tool (CAT).[238] Once a company's privacy policy has been analysed and scored, CAT will

---

[230]ibid 19.

[231]ibid 15.

[232]Privacy Check, https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg (accessed 15 October 2025).

[233]*Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 2.

[234]ibid 3.

[235]ibid 3.

[236]ibid 3.

[237]ibid 2.

[238]*Nokhbeh Zaeem and others*, WI-IAT 2020, 291, 291ff.

also display a chart comparing the achieved score with those obtained by other providers within the same market sector.[239] Furthermore, a list of the top three competitors which have achieved the highest scores regarding GDPR compliance and user control, will be displayed.[240]

With respect to the purpose of this advancement, the creators have stated that whereas the basic version was *"merely aimed to educate and inform users on data practice"*, the competitor analysis functionality *"empowers users to choose services with better privacy policies"*.[241] The idea is that individuals would be able to make a more informed decision in selecting a suitable service provider that combines the desired offering with data processing practices favoured by them. This most certainly supports the data subject in controlling the processing of their personal data and thereby fulfils the function of a Personal Information Management System. The company analysis component is in that sense similar to the PoliCompare functionality offered by Polisis. The crucial difference between those two, however, lies in the fact that PoliCompare requires the user to enter specific URLs of the company's privacy policies they would like to have compared, whereas CAT provides the user with suggestions regarding competitors present on the market. It should therefore be questioned to what extent such propositions constitute a nudge toward the selection of another option and how this affects the roles of the specific parties towards each other. In the same vein as considered in the context of the Usable Privacy Project contemplating the possibilities of nudging users into privacy friendly choices, the question of the existence of an element of active involvement in the decision-making process on the side of the PIMS, needs to be addressed here. By providing the user with an overview of the alternatives available on the market, which, according to the used data mining classification model, are to be considered more privacy friendly, the application is directly nudging the user towards the selection of a different

---

[239]ibid 292.
[240]ibid 292.
[241]ibid 292.

offering. The final decisions will be made by the data subject, most likely also taking into consideration elements other than just privacy. Still, in a sense the PIMS will open the possibility of a completely different data controller being selected in the process. In that sense the influence exerted over the processing activity is even greater, as it does not solely pertain to the configuration of preferences within one service but can potentially shift the entire processing altogether.

Also, since the score provided by CAT is based on the privacy notice of the company and not their actual practices, the consequences of incorrect or incomplete policies, as well as the possibility of producing erroneous scoring results, will become highly relevant as the possibility of a data subject making an adverse decision for their privacy as a result of being misguided cannot be ruled out. While in the context of PoliCompare, those risks have been identified as comparable to those occurring where the individual would have reviewed each policy on their own, the same assumption cannot be made for CAT as it cannot be assumed that the data subject was even aware of the other options. The fact that CAT detects those options independently, in consequence means that the tool is exerting a higher level of influence than a simple comparative function. The central point of this thesis is specifically this level of influence that will become relevant for the determination of the role the Personal Information Management System takes in relation to the data subject. This problem will therefore be further analysed in detail under Part 2 Chapter 4: B. I. Interpretative Tools.

e) Reductive Potential

The here described interpretative tools all pursue the goal of providing truly transparent information to the data subject about the processing of personal data which might concern them. They attempt to alleviate the challenges that individuals face when trying to comprehend typical privacy notices encountered online. With regard to the obstacles identified under Part 1 Chapter 2: B. II. Obstacles, they have the potential to reduce the obstacle of the conflict of objectives (a), as well as inconsistencies (c). While data controllers are by law

required to provide the individual with all the information listed in Articles 13 and 14 of the GDPR, often inescapably leading to lengthy descriptions of the envisaged processing activities, the same does not apply to the PIMS as an intermediary. The presented providers can thereby use this flexibility to reduce the amount of information to those points essential for the interest of the individual, resulting in a more condensed version. Since they do not have an underlying interest in the processing of the individual's information by the controller, they can additionally provide them with an evaluation of the described practices. This is mostly done through the use of simplified, colour-coded risk scores, thereby delivering a clear message as to the extent of the practices, instead of ambiguous and contrived wording.

Interpretative tools also tackle the problem of inconsistencies between privacy policies of different controllers, who all use various forms of presenting the necessary information both visually and linguistically. Since the described systems all automatically analyse existing policies and subsequently present the findings in a standardised, simplified form, users opting for one of these tools will be confronted with one familiar form of presentation, allowing them to become acquainted with the subject matter and thereby over time, gain a deeper understanding for the underlying issue, making the control of one's data a routine task rather than a heavy burden. This standardisation also has the potential of simplifying the comparison of privacy practices of various controllers. Once the obstacle of information being hidden under various headings, sub-sections, FAQs or "learn more" links is removed, the data subject will be able to effortlessly compare and contrast the extent of the described processing activities. Some of the above-mentioned providers of interpretative PIMS have identified that potential as well and added a comparative component to their service offering, at times even directly suggesting more privacy friendly alternatives to the user.

It should, however, be noted that while the described systems have considerable potential when it comes to the reduction of the hindrances of inconsistencies and conflicting objectives for privacy policies, they are not without risks. Most importantly, the analysed

tools will also suffer from the obstacle of either lacking or incorrect information. Since the application solely analyses the existing policies, any inaccuracies or misrepresentations made therein will be automatically transferred onto the PIMS. While the fact that information is missing could be flagged to the data subject, it will not solve the underlying issue. Additionally, the varying degree of accuracy for these systems should not be discounted. While they might be used as a form of support in finding the relevant information in long and complicated privacy policies, making truly relevant decisions on how to handle one's personal data can be potentially risky.

2. Auditing

Auditing tools, while pursuing the same transparency enhancing objectives, focus on different functionalities to do so. Their primary goal is the review of privacy policies regarding their accuracy, as well as legal compliance.

a) MAPS

The Mobile App Privacy Systems (MAPS) has been designed in order to compare the statements made by data controllers within their respective privacy policies, with the actual underlying processing activity.[242] The work conducted on the tool is a part of the previously-mentioned Usable Privacy Project (see Part 1 Chapter 2: B. III. 1. b)) and has been based on earlier analyses performed by the authors.[243] As a first step, MAPS performs a policy analysis through natural language processing and machine learning techniques, similar to the interpretation PIMS described before.[244] It then applies code analysis techniques to verify the app's behaviour.[245]

---

[242] *Zimmeck and others*, PoPETs 2019, 66, 67.

[243] *Zimmeck and others*, in: NDSS Symposium, 1, 1ff; https://cdn.stmarytx.edu/wp-content/uploads/2020/10/GUILeak-Identifying-Privacy-Practices-on-GUI-Based-Data.pdf (accessed: 25 February 2026).

[244] *Zimmeck and others*, PoPETs 2019, 66, 67.

[245] ibid 72-74.

Based on the collected findings, the tool flags potential compliance issues where the application being examined is performing processing activities not disclosed in an appropriate manner.[246] During the first review conducted by the tool, 1,035,853 Android apps from the Google Play Store were evaluated.[247] Out of those, 49.1% did not link to a privacy policy, although the code analysis suggested that most were in fact processing personal data.[248] For those apps containing a privacy notice, a median of three compliance issues per policy was identified.[249]

It is, however, questionable whether MAPS can actually be considered a Personal Information Management System. While the described functionality could most likely be used by individuals in order to verify the correctness of privacy policies for the applications they use, this does not seem to be the intent of the tool. According to the published research, MAPS has been created with the objective of supporting regulatory agencies and app store providers in identifying non-compliant applications.[250] App developers are also mentioned as potential beneficiaries in the sense that the tool could be used to perform compliance checks on their service offering.[251] Data subjects, however, are not included in the list of future users. In that sense, MAPS does not actually *"aim to empower individuals to control the collection and sharing of their personal data"* and cannot formally be considered a Personal Information Management System. Since, however, the here presented examples only serve the purpose of illustrating the different functionalities considered in the context of PIMS and, since the underlying auditing functionality does in fact have that potential, it should therefore still be analysed in the context of this thesis.

---

[246]ibid 74.
[247]ibid 66.
[248]ibid 75
[249]ibid 76.
[250]ibid 80.
[251]ibid 80.

b) AppTrans

AppTrans (Transparency for Android Applications) works to a large extent analogous to MAPS. The two main elements of the tool are (1) an automated analysis of the privacy policy based on machine learning, filtering out which type of personal data is being processed according to the notice provided by the controller; and (2) an analysis of the application's binary code, which detects personal data being collected by the application.[252] The analysis performed by the prototype revealed a high level of non-compliance (59.5%) among the selected applications, which was primarily caused by the collection of data though third party libraries not declared within the policy.[253] Also analogously to MAPS, AppTrans does not identify data subjects as the primary users, but rather focuses on supporting the needs of developers and regulators, in this case even more explicitly so by stating that the goal is to *"show why the emphasis on consumer privacy tools needs to expand to include transparency tools for developers and regulators"*.[254]

c) CLAUDETTE

Much more in line with the "traditional" definition of a Personal Information Management System is the CLAUDETTE (automated CLAUse DETectEr) Project[255], which specifically names empowering the *"civil society representing the interests of consumers"*[256] as its goal, actively asking for *"consumer-empowering AI"*.[257] In contrast to the other presented auditing tools, their research on privacy policies is also explicitly focused on GDPR compliance.[258] In this context, the

---

[252] *Austin and others*, Towards Dynamic Transparency, 15f.
[253] ibid 17.
[254] ibid 9f.
[255] http://claudette.eui.eu/ (accessed: 24 November 2025).
[256] *Contissa and others*, CLAUDETTE meets GDPR, 1.
[257] *Contissa and others*, IJCAI'18, 5150, 5150.
[258] *Liepina and others*, in: ASAIL 2019, 1.

design of a “Golden Standard” for such notices was attempted, the purpose being the creation of a platform that could allow users access to their data and support them in understanding how it is being used, as well as what their rights are towards a specific controller.[259]

At the time of writing, the design of such a tool was still in progress, with the latest publication identifying a number of challenges in developing an automated system able to assess the compliance of a privacy policy within the requirements of the GDPR.[260] These were mainly (1) the inability of an automated detection tool to understand the entire context under which the information was being provided, rather than just analysing a singular sentence; (2) the fact that it would need to understand the difference between a fully informative sentence and one that is missing certain information or phrased too vaguely; and (3) preserving functionality and accuracy across all official languages of the Member States.[261] First analysis performed on the implemented Support Vector Machine-based classifier reportedly showed an encouraging level of precisions and thereby indicating that an automated detection of problematic clauses should be generally feasible.[262] Once the performance level is considered sufficient, the project plans to increase the volume of the dataset and leverage the development of technologies such as scanning tools for supervisory authorities and consumer organisations, consumer-end tools, or web-crawlers.[263] It should also be noted that CLAUDETTE is simultaneously working on the development of a tool for the automated detection of unfair clauses in online consumer contracts.[264] A beta-version where individuals can submit any terms of service for scanning, is already available online.[265]

---

[259]ibid 2f.
[260]ibid 4f.
[261]ibid 4f.
[262]*Contissa and others*, CLAUDETTE meets GDPR, 55.
[263]ibid 59.
[264]*Lippi and others,* in: Legal Knowledge and Information Systems, 145, 145ff.
[265]http://claudette.eui.eu/demo/ (accessed 14 October 2025).

In contrast to MAPS and AppTrans however, CLAUDETTE's auditing functionality is not aimed at reviewing the accuracy of the provided information as it does not possess the means to analyse the actual underlying processing activity. Once functional, it would simply review the legality of the described terms and the quality of the provided information. In that sense, it can also be considered partly interpretative since aspects such as comprehensiveness and clarity of expression are also evaluated.[266] This amalgamation of varying functionalities, purposes and target groups is, however, typical in the current market of Personal Information Management Systems. Since no official definition or standards for these types of applications exist and considering that most are still in the development phase, the ideas behind them and approaches taken to implement those are numerous.

d) Reductive Potential

Whereas interpretative tools are aimed at presenting the information in a more attainable way, in a sense providing the data subject with an "interpretation" of the described data processing practices often in the form of scores, auditing tools focus on reviewing whether the facts presented in the privacy policy are actually accurate or to what extent the presented activities are even lawful. These auditing functionalities primarily have the potential of reducing the obstacle of lacking information identified under Part 1 Chapter 2: B. II. 2.

As discussed above, multiple studies have evidenced that privacy policies, especially in the online environment, often fail to disclose legally required information. Whereas this might be evident to lawyers and experts in the field, this will most likely not be the case for the average consumer. Added to that is the question of the legality of the described processing activity. Since a determination on such a point requires in-depth knowledge of the subject, it would in most instances be virtually impossible for the data subject to identify such

---

[266] *Contissa and others*, CLAUDETTE meets GDPR, 15.

a clause. If, however, a tool was trained to flag issues such as “no legal basis for processing mentioned”, “insufficient information on purposes of processing”, or “illegitimate transfer mechanism”, this could in a sense empower the individual to take further action. An auditing functionality such as this would not be able to make any corrections within the policy but it would definitely raise a certain awareness.

It is also imaginable that a natural person might already suspect the illegitimacy of certain practices but due to a lack of knowledge would feel unsure or insecure to act upon it. Getting a confirmation from a system specifically designed for that purpose might give them the necessary affirmation. This incentive to act is also directly related to the assurance of another data subject right, namely the right to lodge a complaint with a supervisory authority, as defined in Article 77 GDPR. Individuals have the right to involve the DPA where they consider a certain processing activity concerning them to infringe the Regulation. Getting verification from the PIMS as to the potential illegality of a certain practice including the legal basis and reasoning for such a determination, would make it significantly easier to formulate one’s grievance, thereby enabling the data subject to act upon their right.

This element of enablement is even more crucial when it comes to the second auditing functionality of reviewing the correctness of the statements made by the controller within a specific policy. In general, data subjects have no means to verify to what extent claims regarding the ways in which a company handles personal data are in fact true. This not only applies to the online environment, as incorrect or misleading information can be provided under any circumstances. The risks, however, are substantially different. While surfing the internet, users regularly disclose personal information without even being aware of it.[267] This problem does not materialise itself to the same extent offline, as a person has to actively give out information at some point. This data, once collected, can be shared with

---

[267] *Larsson/Jensen-Urstad/Heintz*, 8 CAL 2021, 101, 101ff; *Gomer and others*, IEEE 2013, 549, 550; *Ur and others*, in: SOUPS '12, 1, 6, 9.

third parties as well. The possibilities, however, are limited by basic practical implications. This is why consumers of online services require particular protection. If the PIMS would allow them to verify how their data is in fact handled by a service provider and whether this treatment is in line with the privacy policy, this would again not only raise their awareness, but most importantly establish a solid basis for issuing a complaint with the Data Protection Authority. In that sense, it is very surprising that the currently dominating tools presented above (MAPS and AppTrans) do not seem to consider data subjects their primary audience. While the use of these auditing functionalities by the controllers or the supervisory authorities can be equally beneficial for the end users, there seems to be no reason consumers should not utilise them directly.

3. Responsive

The last type of applications which will be discussed in the context of transparency enhancing technologies at this point, are responsive tools. In a sense, however, these are not necessarily to be seen as a separate type altogether but probably more as a subcategory of the two models presented earlier. The first two types are both directed at the assurance of the data subject's right to receive transparent information, regarding the processing performed on their personal data; however, they focus on different objectives to do so. Whereas interpretative tools aim at presenting the content of privacy policies in a comprehensible format, auditing tools are concerned with reviewing their level of compliance. Responsive tools, on the other hand, do not differ from these two in connection to their goals but rather the presentation of the achieved results. The idea behind such is in essence that the information is being presented to the user in the form of a "response" either to a specific question or concern, thereby seemingly making the experience more interactive on the user's side. It should, however, be noted that responsive tools usually are based on the same underlying technology (namely mainly machine-learning and natural language processing models) as the tools presented above. They might, therefore, still be under development and will lack the necessary maturity level. Still, in spite of their

limited level of applicability and potential hurdles in further progression, the underlying idea is important to note and should be considered as well, due to their focus on communication and user-friendliness.

a) PriBot

PriBot is an automated chatbot answering free form questions about privacy policies.[268] Its functionality is offered jointly with Polisis and PoliCompare (described earlier) and is based on the hierarchical multi-label classification created therein.[269] Once the user copies the URL to the relevant webpage and enters the applicable questions, the machine-learning layer probabilistically annotates the question and the identified policy segments with the privacy categories and attribute-value pairs.[270] The potential answers are subsequently ranked by computing a proximity score.[271] The efficiency of the system is evaluated based on the metrics of predictive accuracy and user-perceived utility.[272] According to the results, PriBot was able to provide a correct answer among its top three results for 82% of the test questions, with at least one of these answers being considered relevant by 89% of the participants.[273]

PriBot is reportedly the first system to offer the user the option to actively communicate with a chatbot and answer specific questions about a particular policy.[274] The idea was inspired by the rise of "conversation-first devices", such as voice-activated digital assistants and smartwatches,[275] as well as the trend of automation in areas such as legal advice, insurance claim resolution, and privacy policy

---

[268] *Harkous and others*, SOUPS 2016, 1.
[269] See Part 1 Chapter 2: B. III. 1. a) Polisis.
[270] *Harkous and others*, USENIX 2018, 531, 539.
[271] ibid.
[272] ibid 540-544.
[273] ibid 531.
[274] ibid 531.
[275] ibid 539.

presentation.[276] To that extent, it is in a sense surprising that this concept, as of now, has not really been furthered within the field. The reason for this might, however, lie in the previously mentioned low level of maturity in some of these systems, as well as the prioritisation of other interactive aspects. It is also possible that privacy-aware users, who constitute the primary audience, might be inclined to be less trusting of such a tool in consideration of the privacy concerns caused by other digital assistants. Still, considering the immense developments in Chatbots, based on generative AI, such as ChatGPT or GPT4, [277] further advances on the front of responsive PIMS are to be expected.

b) Privacy Bird

The second responsive tool discussed is PrivacyBird, a Browser-Helper-Object (BHO) which provides users with a determination on whether the currently used website matches their personal privacy preferences.[278] As a first step, individuals will input their expectations with regard to the treatment of personal data into the tool. Afterwards, a bird-icon will be displayed on the browser title bar, informing the user whether the currently visited website complies with the previously defined preferences.[279] A green bird informs the user that the website's practices match with the expected level of privacy, a yellow bird indicates that the privacy policy cannot be analysed, and a red bird warns the individual that the processing operations go beyond the level declared as acceptable.[280]

While both the underlying idea as well as the design were quite promising, the application did not prevail due to the limited amount

---

[276]ibid 544.

[277]*Helberger/Diakopoulos*, 12 IPR 2023, 1, 2; *Strowel*, 54 IIC 2023, 491, 491; *Hacker/Berz*, 8 ZRP 2023, 226, 226.

[278]Privacy Bird, http://www.privacybird.org/, (accessed: 16 October 2025).

[279]*Cranor/Arjula/Guduru*, in: WPES '02, 1, 3.

[280]*Cranor/Arjula/Guduru*, in: WPES '02, 1, 3.

of privacy policies the tool was able to read.[281] The analysis and matching of the privacy policies is based on the Platform of Privacy Preferences (P3P) format, developed by the World Wide Web Consortium in 2002.[282] The P3P protocol allowed websites to create machine readable declarations regarding the collection and processing of the users' personal data.[283] It was, however, obsoleted in 2018[284] mainly due to an insufficient level of browser implementations.[285]

c) Reductive Potential

As mentioned before, responsive tools follow broadly the same aims as interpretative and auditing applications have, but attempt to achieve those through different modes of presentation and communication. PriBot serves essentially the same function as its counterpart Polisis in that it provides the user with an explanation regarding the processing activities declared by the controller within a privacy policy. The crucial difference of the chatbot functionality, however, lies in the fact that it has the potential of offering the individual exactly the information for which they are looking. The significance of this differentiation should not be underestimated in the sense of its reductive potential, especially with regards to the conflict of objectives. As outlined under Part 1 Chapter 2: B. II. 1., it is virtually impossible for controllers to provide information on all the points required by Article 13 and 14 of the GDPR without creating an elaborate and convoluted declaration. This can, to an extent, be remedied by interpre-

---

[281]One of the most frequently voiced concerns identified in user studies was the fact that the bird would appear yellow on most visited webpages. See: ibid 7.

[282]https://www.w3.org/TR/P3P/ (accessed: 25 February 2026).

[283]For more details on the history and functionality of P3P please refer to: *Cranor*, 10 J. on Telecomm. & High Tech. L. 2017, 273, 279 -282; *Hochheiser*, 2 ACM Trans. Internet Technol. 2002, 276, 267ff.

[284]https://www.w3.org/TR/P3P/ (accessed: 25 February 2026).

[285]https://www.w3.org/TR/P3P/ (accessed: 25 February 2026). See also: https://cdt.org/wp-content/uploads/pdfs/P3P_Retro_Final_0.pdf (accessed 29 January 2026).

tative tools and by standardising and condensing the presented information. The reduction of the policy to certain elements typically deemed as crucial comes, however, at the expense of completeness especially for individuals interested in less common details regarding the processing activity in question. Applications reacting to a specific question or request of the data subjects, on the other hand, have the crucial potential of bridging that gap.

A similar possibility can be seen in the solution proposed by Privacy Bird. Since the users specifically set up their personal privacy preferences in advance, the tool only needs to react to those elements deemed as essential by the data subject. Another advantage lies in the fact that the displayed icon keeps the user constantly aware of privacy related issues. Whereas the other discussed tools might provide more in-depth analysis of the processing activities, the data subject needs to actively use these in order to obtain the relevant information. Here, however, even an individual who might at the moment be focused on something else or whose interest in data privacy might have diminished, will be alerted when entering a website that does not adhere to their choices. Considering the potential displayed by these tools in further reducing the hindrances of the provision of transparent information as well as their interesting design, it is to an extent surprising that solutions such as these have not found more general recognition within the field of transparency enhancing technologies. While responsive tools might not yet have risen to the position of market leaders they should, however, still be considered in the context of possible functionalities of Personal Information Management Systems and their further development not ruled out.

4. Interim Conclusions: Information

The second type of functionalities of Personal Information Management Systems, which have been analysed relate to the provision of information as required by Articles 13 and 14 of the GDPR, which stems directly from the principle of transparency as laid down in Article 5(1)(a). The previous section provides an overview of the requirements put on controllers regarding the provision of information

to the data subject, including both the timeline and the way the relevant facts need to be presented. Subsequently, currently applicable practical hindrances in achieving that goal, namely (1) the inherent conflict of objectives originating from the regulation; (2) the problem of incomplete and incorrect privacy notices; and (3) the extreme differences in both visual and textual presentations of facts by different service providers were identified. As a next step, both existing and potential functionalities offered by Personal Information Management Systems, which have the potential to alleviate some of these issues, were presented. These were broadly classified into interpretative, auditing, and responsive tools.

It has been established that interpretative tools have considerable potential in reducing the hindrances of inconsistencies and conflicting objectives for privacy policies as they allow the presentation of the relevant information in a standardised and simplified form, at times even offering an assessment on the controllers' practices. They are, however, subject to the risk of underlying inaccuracies and misrepresentations in the reviewed policies as these would automatically be transferred onto the analysis provided to the data subject. This inherent risk can be partially remedied through the use of auditing tools which can compare the actual processing being performed by an application or webpage, with statements made by the controller about their privacy policy. This service, alongside the possibility to review the legality of these policies, might also support users in the enactment of their right to lodge a complaint with the supervisory authority in accordance with Article 77 GDPR. Last but not least, responsive tools add the capability of reacting to the needs of the individual by only providing the information specifically being requested, thereby increasing the focus of the provided facts. By enabling the individual to understand various aspects of the processing activity in question, the described functionalities thereby support the data subject in the gaining more control over their personal data, including them into the scope of Personal Information Management Systems.

C. Consent

The third functionality which will be discussed as part of this chapter refers to the topic of consent. Consent, as such, does not constitute a principle of data protection nor is a data subject right. Formally speaking, it is simply one of six basis legal bases for the processing of personal data laid down in Article 6. Still, its relevance in the field of data privacy in general, as well as in the context of Personal Information Management Systems, can hardly be overemphasised. The reasons for this are multiple but based on the view presented here can be distilled into two main justifications.

First, consent constitutes the legal basis of which the data subject is most in control. The provision of consent requires an action from the individual acknowledging the actual processing activity in question, whereas in the case of all other legal bases, processing can, to a large extent, occur without the individual's knowledge and certainly without their agreement. In that sense, it is the ultimate embodiment of power which can be exercised by the data subject, since the possibility of applying this legal basis by the controller is, at least in theory, only dependent on their will.[286] Consequently, a consent feature can be considered the ultimate functionality of a Personal Information Management System, as the whole purpose of such is the facilitation of control by the data subject.

The second reason for which consent has such a high relevance in the field of data privacy connects to the fact that it is unfortunately inherently flawed. The General Data Protection Regulation sets out a number of requirements necessary for the obtaining of valid consent from a data subject. Controllers, however, regularly fail to meet this, either because of organisational deficiencies or at times even bad faith. [287] There is also a large area of more or less ambiguous practices applied by business, which are implemented in order to

---

[286]Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 176; *EDPB*, Guidelines 05/2020, para 3; *Buchner/Kühling*, 41 DuD 2017, 544, 545.

[287]*Zimmer*, Streamingplattformen, 9f.

have individuals agree to the use of their personal data.[288] Their legality is, however, constantly questioned by legal professionals as well as the Data Protection Authorities.[289] Additionally, users report both frustration and difficulties in handling the requests they receive on a regular basis. [290] All of these issues and requirements have already been highly debated under the Data Protection Directive and have only gained more relevance over the years.[291] These problems, which will be outlined in detail subsequently, also create an enormous field for improvement. In this sense, the idea of introducing consent tools designed to fix these issues has been subject to much interest within the industry, as of now making them the most developed of all Personal Information Management Systems. All of these issues, as well as the proposed solutions, shall therefore be analysed in this thesis.

I. General Requirements

Before starting a discussion regarding the various problems and obstacles that may result when attempting to obtain valid consent from an individual, the general requirements for consent as set out by the GDPR will be briefly discussed. While Article 6 establishes its status as a legal basis for processing personal data, it does not provide for any further details on how it should be collected. These are respectively found in Articles 4(11), 7 and 8 of the GDPR. First and foremost, Art. 4(11) defines consent as *"any freely given, specific,*

---

[288] *Bermejo Fernandez and others*, 5 Proc. ACM Hum.-Comput. Interact. 2021, 1, 1ff; *Christine Utz and others*, 'CCS '19, 973, 976-982; *Bösch/Erb/Kargl/Kopp/Pfattheicher*, PoPETs 2016, 237, 237ff.

[289] *Nouwens and others*, CHI '20, 1, 2; *Waldman*, 31 Current Opinion in Psychology 2020, 105, 107.

[290] *Choi/Park/Jung*, 81 Comput. Hum. Behav. 2018, 42, 42ff; *Tian/Chen/Zhang*, 12 Applied Sciences 2022, 9702, 4.

[291] *Kamp/Rost*, 37 DuD 2013, 80, 80-83; *Hacker*, Datenprivatrecht, 255-258; *Efroni and others*, 5 EDPL 2019, 352, 355-357; *Blume*, 2 IDPL 2012, 26, 29; *Hermstrüwer*, Selbstgefährdung, 227ff; *Koops*, 4 IDPL 2014, 250, 251ff.

informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". There are therefore four main elements outlined therein necessary for the realisation of consent. It needs to be 1. freely given; 2. specific; 3. informed; and 4. unambiguous.

1. Freely Given

This criterion requires the data subject to have a free and genuine choice whether to agree to a certain processing activity.[292] This also means that there should be no negative consequences tied to the refusal of such.[293] While assessing to what extent the action of a certain individual was in fact free, the overall circumstances under which consent has been provided need to be considered, as well as the particular situation of the person in question. In that context, there are certain typical characteristics which give rise to the assumption that consent was not, or at least not entirely free.

a) Imbalance of Powers

The first element which would prevent an individual's action being considered as free refers to the imbalance of powers between the controller and the data subject.[294] This understanding is also supported by Recital 43 which stipulates *that consent cannot provide a valid legal basis for the processing of personal data, where a "clear imbalance" exists between the parties.* This means, however, that

---

[292]Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 182; *EDPB*, Guidelines 05/2020, para 13; Ehmann/Selmayr / *Heberlein*, Art. 6, para 13f; Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 41.

[293]Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 182; *EDPB*, Guidelines 05/2020, para 13; Ehmann/Selmayr / *Heberlein*, Art. 6, para 13f; Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 41.

[294]Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 42; *Schneide/Härting*, 5 ZD 2012, 199, 201f; *EDPB*, Guidelines 05/2020, para 16-24; *Voigt/von dem Bussche*, GDPR, 95.

the basic “imbalance of powers”, which is often described as being a general factor in any relationship between businesses and consumers, is not sufficient to deny the possibility of obtaining consent.[295] Otherwise, the whole existence of such would, after all, be to a large extent superfluous. As an example of instances in which a clear imbalance can be assumed, Recital 43 mentions scenarios in which the controller is a public authority. This, however, does not mean that such entities are never allowed the use of consent as a legal basis but rather that the relationship between them and any natural person will be subject to more scrutiny.[296] This approach was recently evidenced in the ruling of the Court of Justice of the European Union (CJEU) in the case of *Meta vs. Bundeskartellamt*.[297] The court pointed out that where a social network operator holds a dominant position on the market, this may create a clear imbalance between the parties in the meaning of Recital 43 GDPR.[298] Still, it was concluded that this fact did not automatically prevent the possibility of collecting valid consent from the users of that social network.[299] Users must, however, be able to freely refuse their consent without the need to entirely refrain from the service.[300] In such instances, consent may thereby still be valid, in spite of the potentially dominant position of the controller, since the user would be given a genuinely free choice.

Another example typically provided in this context is the relationship between employers and employees, since these are also subject to an underlying dependency.[301] After all, it would not be entirely

---

[295]Wolff/Brink/v. Ungern-Sternberg / *Albers/Veit*, Art. 6 DSGVO, para 31.

[296]*EDPB*, Guidelines 05/2020, para 17; Wolff/Brink/v. Ungern-Sternberg / *Albers/Veit*, Art. 6 DSGVO, para 31.

[297]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

[298]ibid para 149.

[299]ibid para 147.

[300]ibid para 150.

[301]Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 71; *EDPB*, Guidelines 05/2020, para 21f; Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 44; Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 182. Interesting in that context is however the

unreasonable for an employee to assume that refusing to agree to certain actions might be construed as a lack of loyalty or commitment towards the company.[302] In that sense, even in minor instances, it might be safer to assume a lack of entirely free will on the side of the data subject. If, on the other hand, it is clear that the business does not have any underlying interest in the performance of the processing activity (e.g. employees deciding to sign up for a gym membership or other programmes sponsored by the company, or deciding to post information on the company's intranet page) it can mostly be assumed that no pressure is being put on the employee and their actions are therefore free. German lawmakers have even explicitly set out criteria for the collection of consent from employees in §26(2) of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG). The second sentence therein provides that consent may especially be considered as "freely given" where it is connected to a legal or economic benefit on the side of the employee, or where both parties pursue the same interests. Again, however, the determination of this factor will depend on the specific circumstances at hand.[303] If, for example, all individuals in a company knew that the CEO really wanted people to join the previously mentioned gym membership, the validity of their consent might be questioned, even for this seemingly uncritical activity.

---

fact, that the reference to a clear imbalance of powers in the employment relationship, was in fact included in earlier drafts of the GDPR, but had been deleted in the final version. See: *Freiherr von dem Bussche/Zeiter/Brombach*, 23 [2016] DB 2016, 1359, 1363; *Gierschmann*, 2 ZD 2016, 51, 54.

[302] *Ernst*, 3 ZD 2017, 110, 112; Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 71; Regarding the position of an employee towards their employer see also: Joined cases C-397/01 to C-403/01 *Pfeiffer and others* [2004] ECLI:EU:C:2004:584 para 82: *"[...]the worker must be regarded as the weaker party to the employment contract and it is therefore necessary to prevent the employer being in a position to disregard the intentions of the other party to the contract or to impose on that party a restriction of his rights without him having expressly given his consent in that regard."*

[303] *Ernst*, 3 ZD 2017, 110, 111f; *EDPB*, Guidelines 05/2020, para 22; Sydow/Marsch / *Tiedemann*, §26, para 39.

Interesting here is the question as to how this criterion affects the potential collection of consent via PIMS. On the one hand, potential power imbalances between the PIMS provider and the user might be considered, especially where such a platform would hold significant market power. While at the moment there is no consent management platform holding such power, this is at least imaginable. It should, however, be noted that users will typically be left with at least one viable alternative: namely providing their consent directly to the data controller, instead of using the platform. In that sense, regardless of the specific PIMS business model or their level of market power, the data subject will in principle always be left with the possibility of reaching the same goal while refraining from the use of the service. As a result, the materialisation of a significant imbalance of powers is hard to imagine unless the use of the platform was accompanied by other (for example financial) advantages. Here the specific circumstances, as well as the level of "detriment" resulting for the individual user, would need to be accounted for.

On the other hand, the effect of the consent management platform on the relationship between the data subject and the end data controller could be explored. After all, it is the explicit purpose of PIMS to mitigate certain power imbalances between the different parties.[304] A reduction of any imbalances, or feeling of compulsion on the side of the data subject might, for example, be facilitated through the assurance of anonymity. This form of mitigating imbalances is already practiced in the context of employee consent. Many programmes offering benefits to employees (support in child care, psychological support, gym-memberships) adhere to strict anonymity policies where the employer is only presented with information about the amount and type of services provided, without knowing which individuals took advantage of them.[305] A similar notion could be applied

---

[304] *Attoresi/Moraes*, TechDispatch #3/2020, 2; *Riechert/Richter*, Was die DSGVO braucht, 8-10; *EDPS*, Opinion 9/2016, para 25-28.

[305] For example: AWO Lifebalance FAQ, https://www.awo-lifebalance.de/unsere-dienstleistungen/faq (accessed: 24 October 2025); PME Familienservice FAQ, https://mein.familienservice.de/faq (accessed 24 October 2025).

for PIMS. As a result, the controller would not be able to differentiate between different data subjects based on the type of consent they provided. The individual would therefore not feel pressured, either directly or indirectly, to agree to any processing activities they might feel uncomfortable with. This would also be beneficial to the controller, as they could effectively prove that data subjects could choose freely without fearing any detriment. After all, the principle of accountability (Art. 5(2) GDPR) clearly establishes that they need to prove that all of the conditions under the GDPR are in fact met.

b) Conditionality

The second element preventing the provision of truly "free" consent is outlined in Art. 7(4), which states that in that context, it should be taken into account whether the performance of a contract or the provisions of a service are being made conditional on the consent to the processing of personal data. This factor, also referred to as "bundling", underlines the necessity of a clear differentiation between the legal basis of Art. 6(a) and (b).[306] In this sense, any processing of personal data which is in fact necessary for the performance of a contract the data subject wishes to enter into, should be strictly based on Art. 6(b).[307] Where the controller has an interest in collecting additional information about the data subject and wants to do so based on the individual's consent, the provision of such cannot be treated as a prerequisite for providing the desired service. This is also again supported by Recital 43, which states that in such instances, consent would be "presumed not to be freely given". This is also referred to as a vertical restriction of interconnection.[308]

It is however important to note that Art. 7(4) does not contain an absolute prohibition of these practices as the wording only asks for

---

[306]Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 182; *EDPB*, Guidelines 05/2020, para 26.

[307]*Bühler*, 1 Freilaw 2019, 25, 28; *EDPB*, Guidelines 05/2020, para 30.

[308]Rücker/Kugler, *Dienst*, C. Lawful processing, para 448.

"utmost account" to be taken of the presence of such a bundling when assessing the validity of the consent.[309] This means that, in certain instances, conditionality would still be permissible. What is not clear, on the other hand, is when and to what extent. This question has in fact been the subject of a heated, ongoing debate within the field of data privacy, with some supporting a very strict limitation of such cases[310] and others taking a more flexible approach[311] allowing for many factors such as the market position of the controller,[312] the extent to which other alternatives are available,[313] or the criticality of the offered services[314] to be taken into account.[315] The CJEU has unfortunately not provided any significant guidance on the subject to date. While the topic was briefly brought up in the context of the Planet 49 ruling, the court concluded that since the referring court had not raised a question regarding the compatibility with the requirement of "freely given" consent in that case, it would be inappropriate to provide their opinion on that.[316] The Advocate General Maciej Szpunar, however, touched upon the issue in his Opinion, noting that consent should not only be active but also separate. "It appears to me doubtful that a bundle of expressions of intention, which would include the giving of consent, would be in conformity with the notion

---

[309]*Schätzle*, 5 PinG 2017, 203, 203f; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 7, para 100; *Schantz*, 26 NJW 2016, 1841, 1845; *Bühler*, 1 Freilaw 2019, 25, 28.

[310]*Dammann*, 7 ZD 2016, 307, 311; *EDPB*, Guidelines 05/2020, para 35.

[311]*Schätzle*, 5 PinG 2017, 203, 203ff; *Gierschmann*, 2 ZD 2016, 51, 54.

[312]*Golland*, 3 MMR 2018, 130, 132-133; *Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 555; *Gierschmann*, 2 ZD 2016, 51, 54.

[313]*Baumann/Alexiou*, 7 ZD 2021, 349, 352; Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 52-53a; Wolff/Brink/v. Ungern-Sternberg / *Stemmer*, Art. 7 DSGVO, para 48.

[313] Ehmann/Selmayr, *Heckmann/Pascke*, Art. 7, para 104; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 61.

[314]Ehmann/Selmayr, *Heckmann/Pascke*, Art. 7, para 104; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 61.

[315]For a detailed overview of legal disputes and questions discussed in the context of conditionality refer to: *Hacker*, Datenprivatrecht, 181-195.

[316]Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 64.

of consent".[317] Nonetheless, for the specific case at hand in which a check box required participants to agree to marketing emails from multiple sponsors in order to participate in a lottery, the AG came to the conclusion that such a practice was most likely valid. This assumption was made based on the fact that "the underlying purpose in the participation in the lottery is the 'selling' of personal data".[318] In that sense, Szpunar supported the opinion that the provision of personal data constituted the main obligation of individual in order to allow their participation.[319]

The findings of the Advocate General are relevant on multiple levels. On the one hand, they provide greater insight into the general reading of Art. 7(4). Most importantly, however, they seem to directly support the idea of the business model in which the provision of personal data is used as a form of compensation. This is crucial considering their popularity in the current market economy.[320] Moreover, these models come in multiple variations, with some entirely financed through data collection, some offering both a "free" and a superior "premium" version ("freemium" models), and others still requiring traditional payment but offering special bonuses or discounts for the provision of one's personal data.[321] The lack of a specific regulation of such is, however, also a cause for the emergence of multiple legal questions regarding the basis of their functioning, their doctrinal qualification, their placement in the national legal systems, as well as their implications with regard to consumer protection.[322] Further aggravating those issues of classification is the fact that most of these

---

[317]Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, Opinion of the AG Szpunar, para 66.

[318]ibid para 99.

[319]ibid para 99.

[320]*Stock*, 8 JISTaP 2020, 6, 6ff; *Nolte*, in: Bus. Info. Sys., 273, 273ff; *Lubasz/Davida*, in: New Legal Reality, 521, 521ff; *Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 551-556.

[321]*Hacker*, 2 ZfPW 2019 148, 154-157.

[322]*Langhanke/Schmidt-Kessel*, 4 EuCML 2015, 218, 218ff; *Lubasz/Davida*, in: New Legal Reality, 521, 521ff; *Hacker*, 2 ZfPW 2019 148, 148ff; *Wendehorst/Graf von Westphalen,* 52 NJW 2016, 3745, 3748ff; *Metzger*, 6 AcP 2016, 817, 817ff.

are explicitly sold as "free", not disclosing the fact that data is used to finance their business model and that this constitutes a necessary element of such.[323] In that context, such services are largely subject to criticism from experts in the field of data privacy, as they are accused of effectively forcing individuals into the disclosure of their personal information.[324] Others, however, argue that an excessively strict reading of Art. 7(4) rendering such services invalid, would in fact have the effect of taking away the data subjects' right to self-determination, in a sense prohibiting them from making their own decision regarding the use (or rather selling) of their personal data.[325]

An interesting factor to be considered in that context is the inclusion of services where digital content or a digital service are being supplied to the consumer and the consumer provides to the trader their personal data under the scope of the Digital Content Directive.[326] While this is in principle to be considered a welcome addition, the final text is in fact far vaguer than initially intended. The first proposal, after all, explicitly referred to the provision of personal (or other) data as an exchange for the receipt of digital content.[327] This was, however, amended based on substantial criticism from the European Data Protection Supervisor, who underlined the fact that since the protection of personal data is considered a fundamental

---

[323] *Schmidt-Kessel/Grimm*, 1 ZfPW 2017, 84, 84 ff; *Langhanke/Schmidt-Kessel*, 4 EuCML 2015, 218, 218.

[324] *Zuiderveen Borgesius/Helberger/Reyna*, 54 CMLRev. 2017, 1427, 1444.

[325] *Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 556; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 60.

[326] See Art. 3(1) of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[327] Art. 3(1) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final - 2015/0287 (COD): „*This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data*".

right, it should not be considered as a commodity.[328] This is why the final version leaves open whether the provided data is in fact considered as compensation, opening the doors for national transposition to regulate this fact.[329] In that sense, the debate on these business models is far from completed and will most likely continue to be relevant for the foreseeable future. The idea of using personal data as an equivalent for monetary compensation will also further come into play in the context of Personal Information Management Systems, as there are certain tools which specifically market themselves as enabling users to generate financial gains for their data. This should, however, be discussed in more detail subsequently.

c) Granularity

The third element necessary for the assurance of "free" consent also refers to a form of bundling, which in this context prohibits the combination of multiple purposes.[330] This factor, also referred to as granularity or a horizontal restriction of interconnection, requires that where consent is being collected for multiple purposes at once, individuals should be given the option to only select the operations they wish to agree to, omitting others.[331] This condition is also outlined in Recital 44 which states that "[c]onsent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case". The importance of this element has also recently been underlined by the CJEU in the Case of Meta vs. Bundeskartellamt, where the court concluded that data subjects should

---

[328] *EDPS*, Opinion 4/2017, para 14.

[329] *Hacker*, 2 ZfPW 2019 148, 165.

[330] *EDPB*, Guidelines 05/2020, para 42; *Brüggemann/Hötzel*, in: Sozialdatenschutz in der Praxis, para 111f; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 6; Rücker/Kugler, *Dienst*, C. Lawful processing, para 448.

[331] ibid.

be given the possibility *of providing separate consent for the processing of data within the network and so called "of Facebook" data collection.*[332]

It is, however, important to note that the granular provision of consent should not pose a hindrance to the general intelligibility of the provided information. Where an overly detailed outlining of purposes would have such an effect, a compromise between the conflicting aims will need to be found. [333] Personal Information Management Systems might be helpful in two ways in that regard. First, they could allow an adjustment of the level of granularity based on specific user preferences. While a facilitation of such a personalisation might not be economically feasible for a single controller, the cost-benefit analysis would likely come to a different conclusion for a specialised tool providing this option for a large range of controllers. Furthermore, standardisation has been proven to improve the intelligibility of notices.[334] Based on that, a more granular presentation of the available option might be possible, in which the PIMS ensures that all privacy notices are being presented in a similar manner.

d) Detriment

Furthermore, Recital 42 outlines that "[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment". This means that whenever an individual has to fear that their refusal to agree to a certain processing activity might result in negative consequences for them, it cannot be assumed that they have acted

---

[332]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 151.

[333]*Hermstrüwer*, Selbstgefährdung, 88; *Kamps/Schneider*, 1 K&R-Beilage 2017, 24, 25; *Hacker*, Datenprivatrecht, 155; Kühling/Buchner / *Bäcker*, Art. 12, para 12; *Gluck and others*, SOUPS '16, 321, 322.

[334]*Karegar/Pettersson/Fischer-Hübner*, 23 ACM Trans. Priv. Secur. 2020, 1,, 35.

based on their own free will.[335] The European Data Protection Board lists consequences such as deception, intimidation, and coercion as examples of such detriment[336] but also refers to the fact that the incurring of costs could be considered a disadvantage.[337] Such a broad understanding would, however, again have the potential of invalidating the previously mentioned business models, in which individuals choose to "pay" with their personal data, especially if a more privacy friendly alternative was only available under the condition of additional fees.[338] This restrictive interpretation would in turn take away the free choice of the individual to select the provision of data, rather than payment for a service.[339] On the other hand, the extent to which the choice is in fact free would also depend on the financial circumstances of the person in question who might be indirectly forced to the disclosure of their personal data where financial hardship does not allow them the acquisition of the "premium" version. To that extent, the availability of reasonable alternatives and the overall importance of the service will most likely need to be considered when determining whether the denial of a certain service or its part would in fact be considered detrimental.[340]

The debate on these types of "freemium" or "pay for privacy" models, has recently gained even more practical significance as a result of the CJEU ruling in the case of *Meta vs. Bundeskartellamt*.[341] Here the Court supported the notion that it is essential for users to have

---

[335]Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 68; *EDPB*, Guidelines 05/2020, para 46ff; *Ernst*, 3 ZD 2017, 110, 112.

[336]*EDPB*, Guidelines 05/2020, para 47.

[337]*EDPB*, Guidelines 05/2020, para 46.

[338]*Bühler*, 1 Freilaw 2019, 25, 27f.

[339]*Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 556; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 60.

[340]*Hacker*, Datenprivatrecht, 189f; *Baumann/Alexiou*, 7 ZD 2021, 349, 352; Wolff/Brink/v. Ungern-Sternberg / *Stemmer*, Art. 7 DSGVO, para 48; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 7, para 104; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 61.

[341]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

the option to decline processing activities which are not strictly necessary for the performance of the contract, without being excluded from the platform.[342] Such users should rather be offered an equivalent alternative, free of these processing operations.[343] However, the Court also stated that such equivalent alternatives may be provided *"if necessary for an appropriate fee",*[344] thereby explicitly supporting the idea of "pay for privacy" models. As a result, Meta has now included such a fee for individuals who opt-out of certain processing activities, giving new force to the old debate.[345] While the prevailing opinion still seems to generally support the validity of such solutions,[346] there are also those clearly arguing against it.[347] Recently, 28 NGOs issued an open letter to the European Data Protection Board asking it to oppose this "pay or ok" approach.[348] If such models are allowed, the question occurs what type of fee should be deemed

---

[342]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 150.

[343]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 150.

[344]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 150.

[345]https://verfassungsblog.de/competition-law-as-a-powerful-tool-for-effective-enforcement-of-the-gdpr/ (accessed 26 February 2026); https://www.salinger-privacy.com.au/2020/09/28/paying-for-privacy/ (accessed 07 March 2026); https://www.wired.com/story/meta-facebook-pay-for-privacy-europe/ (accessed: 25 February 2026); noyb, 'Meta (Facebook / Instagram) to move to a "Pay for your Rights" approach', https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach, 3 October 2023 (accessed: 16 October 2025).

[346]https://verfassungsblog.de/competition-law-as-a-powerful-tool-for-effective-enforcement-of-the-gdpr/ (accessed 26 February 2026); *Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 556; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 60.

[347]https://www.salingerprivacy.com.au/2020/09/28/paying-for-privacy/ (accessed 07 March 2026); noyb, 'Meta (Facebook / Instagram) to move to a "Pay for your Rights" approach', https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach, 3 October 2023 (accessed: 16 October 2025).

[348]Letter to the EDPB: 'Pay or okay' – the end of a 'genuine and free choice', https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf, 16 February 2024 (accessed 16 October 2025).

"appropriate" for the resignation of one's fundamental right to privacy. Most seem to argue for an amount which is low enough so that it would not be deemed as a detriment to the individual user.[349] This approach, however, creates the need for making an essentially impossible determination as depending on the individual's financial situation; any amount no matter how low could have the potential of being "too high" for a specific person. It also fails to take into account the potential cumulation of various "privacy fees" of different providers over time.[350] As a result, groups who are already economically disadvantaged run the risk of being even further marginalised.[351] The possibility of obtaining a more privacy friendly service based on payment alone should therefore categorically be excluded if no other options are available to the data subject.

The exclusion of monetary payment for the refusal of consent in the context of social networking sites and other similar services should, however, not lead to the conclusion that PIMS would need to be offered for free. The intention of a PIMS is to enhance the level of control and privacy on the individual's side. In that sense, the user would be "paying for privacy". Here, however, the protection of privacy is an essential part of the service. PIMS are therefore not to be equated with "pay for privacy" models, but rather "Privacy as a Service".[352] Unless the PIMS therefore intended to use the individual's personal data for other purposes than the provision of services, the restriction of Art. 7(4) GDPR would not apply as Art. 6(1)(b) would be used as a legal basis for the required processing.

---

[349]*Hacker*, Datenprivatrecht, 190; *Krohm/Müller-Peltzer*, 12 ZD 2017, 551, 553; *Golland*, 3 MMR 2018, 130, 134.

[349]Letter to the EDPB: 'Pay or okay' – the end of a 'genuine and free choice', https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf, 16 February 2024 (accessed 16 October 2025).

[350]ibid.

[351]https://www.salingerprivacy.com.au/2020/09/28/paying-for-privacy/ (accessed 07 March 2026).

[352]*Itani/Kayssi/Chehab*, DASC '09, 711, 711 ff; *Su/Hyysalo/Rautiainen/Riekki/Sauvola/Maarala/Hirvonsaloi/Li/Honko*, 49 Computer 2016, 49, 49ff.

2. Specific

The second requirement outlined by Art. 4 No. 11 for validity of consent directly relates to the principle of purpose limitation found in Art. 5(1)(b) and requires the authorisation provided by the individual to refer to a specific processing activity performed for explicitly outlined purposes.[353] This is primarily necessary in order to avoid the collection of too generalised statements, allowing the processing of personal data for an unlimited number of reasons or time.[354] This phenomenon is also commonly known as a "function creep", meaning a service which collects consent for a very generalised purpose and based on that, processes it in forms which were not initially anticipated by the data subject.[355] This is also supported by Recital 32, which provides that where a processing operation has more than one purpose, each of these would have to be authorised by the data subject. The significance of this criterion is also not to be underestimated, as considerations on the specificity of the users' consent were in fact also part of the reasoning for one of the biggest fines issued by the National Commission on Informatics and Liberty (CNIL) to date.[356] It is in that crucial context that the authorisation of the individual corresponds to each specific element concerning the processing activity, such as the set of personal data, the controller, the planned actions, the purposes, and the recipients etc.[357] Any change

---

[353]Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 183; *EDPB*, Guidelines 05/2020, para 55-61; Rücker/Kugler, *Dienst*, C. Lawful processing, para 450.

[354]Rücker/Kugler, *Dienst*, C. Lawful processing, para 450.

[355]*Westphal*, 18 EuZW 2006, 555, 560; *Stoklas*, 15 ZD-Aktuell 2018, 06268; *EDPB*, Guidelines 05/2020, para 56.

[356]CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC' para 157, https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf (accessed: 22 October 2025): *„The specific nature of the consent is not respected because the user, through these actions, accepts all of the processing of personal data implemented by the company as a block, including personalised advertising.".*

[357]*Voigt/von dem Bussche*, GDPR, 96; *Piltz*, 9 K&R 2016, 557, 563; *Gierschmann*, 2 ZD 2016, 51, 54; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 68.

regarding one of the agreed upon characteristics would in turn require a separate agreement from the data subject.

This condition is one of the main reasons why the validity of consent management platforms in general is being seriously questioned within legal literature.[358] The problem is that the PIMS will still need to obtain specific consent for each processing activity of each separate controller. [359] Any type of general authorisations such as "always agree to US data transfers" or "always agree to processing for research purposes" would, on the other hand, be invalid based on this criterion. This raises the question of the extent of their practical use. After all, many individuals likely hope for a type of technology that would decline or accept cookies for them automatically without the need to set-up preferences for each individual website. Still while subject to some restrictions, valid consent meeting all of the legal requirements can still be collected through a PIMS. Some have also suggested the introduction of an EU-wide extension of the concept of "broad consent" is in order to allow for a more efficient functioning of consent management platforms.[360] Others have also pointed out that an overly restrictive reading of this requirement would lead to paradoxical results and can thereby not be supported.[361] Prohibiting the data subject from any level of generalisation where consent is being provided by technical means, would essentially be equivalent to forcing them to deal with questions they explicitly do not wish to be confronted with, thereby directly going against the purpose of the Regulation.[362] This line of argumentation makes even more sense if

---

[358] *Hanloser*, 8 ZD 2023, 421, 421; *Schmitz*, 14 ZD-Aktuell 2023, 01304; Assion / *Aretz*, § 26 TTDSG, para 17; different opinion, however, in: Geppert/Schütz / *Schmitz*, TTDSG §26, para 7-13; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 16.

[359] *Voigt/von dem Bussche*, GDPR, 96; *Piltz*, 9 K&R 2016, 557, 563; *Gierschmann*, 2 ZD 2016, 51, 54; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 68.

[360] *Hanloser*, 8 ZD 2023, 421, 421; Assion / *Aretz*, § 26 TTDSG, para 17; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 16.

[361] *Hacker*, Datenprivatrecht, 607.

[362] *Hacker*, Datenprivatrecht, 607.

we consider the fact that such a demand is also unlikely to lead to any meaningful results. From a practical standpoint, it can be assumed that those individuals who simply want to reject or accept all types of cookies without any differentiation will interact in the exact same way with any cookie banner they encounter. The result would therefore be essentially the same as if a PIMS rejected or accepted all of those cookies in their name but would alleviate the burden from the data subject. Furthermore, for those who do wish to make some specification, the PIMS would likely be more efficient in executing those, since the individual will not always have the time to go into the setting found in the second or third layer of a privacy notice. In that sense, the requirement for consent to be "specific" includes the option for the individual user to "specifically" generalise their consent preferences.

3. Informed

In order to be able to agree to a certain processing activity, the data subject also needs to be provided with a sufficient amount of information regarding such, so that they have the ability to understand the overall circumstances surrounding the processing of personal data, the actual activities, as well as the potential consequences resulting from their agreement.[363] This prerequisite directly relates to the principle of transparency outlined under Art. 5(1)(a), as well as to the right to be informed, as analysed previously (see Part 1 Chapter 2: B. Information).

---

[363] *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 72; Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 183f; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 11 DSGVO, para 8; Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 79.

a) Content

The first question which comes to mind in that context is what types of information would in fact need to be provided by the controller in order to consider a decision of the data subject to be sufficiently informed. Recital 42 puts forwards very minimal requirements, only stating that the individual should be aware of the identity of the controller and the purposes of processing. This will, however, most likely only suffice for the making of an informed decision in very limited circumstances. On the other side of the spectrum, Art. 13 and 14 contain a long list of information to be provided to the data subject as a part of their general right to be informed, regardless of the legal basis of processing.[364] Whether all of this information formally needs to be made available at the time of obtaining consent from the data subject is still subject to debate.[365] Since, however, the legal obligation to provide these details applies either way, it might therefore be most reasonable, as well as efficient, to do so right at the moment of requesting authorisation for the processing activity.[366] While an explicit statement on the subject has not yet been made by the CJEU, the court did not seem to differentiate between the general information requirements and the prerequisite of informed consent in the ruling of Planet 49.[367]

On the other hand, providing individuals with long privacy notices is known to have a negative effect on the users' actual understanding as they are often overwhelmed by the excessive amount of information.[368] This phenomenon is also generally known in other areas

---

[364]See Part 1 Chapter 2: B. I. General Requirements.

[365]*Hacker*, Datenprivatrecht, 174; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 73f; *Ernst*, 3 ZD 2017, 110, 113; Rücker/Kugler, *Dienst*, C. Lawful processing, para 452; Sydow/Marsch / *Ingold*, Art. 7, para 35.

[366]Rücker/Kugler, *Dienst*, C. Lawful processing, para 452.

[367]Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 76-81.

[368]*van Ooijen/Vrabec*, 42 J Consum Policy 2019, 91, 94f; *Monteleone*, 43 Syracuse J. Int'l L. & Com. 2015, 69, 103-109; *Ernst*, 3 ZD 2017, 110, 113.

such as marketing and referred to as "information overload".[369] In this sense, the implementation of such solutions as layered privacy notices, icons, push and pull notices, QR-codes, and other similar best practices already outlined under Part 1 Chapter 2: B. II. 1. Conflict of Objectives might be required. Considering the current uncertainties with regard to the exact formally required content, most controllers, at least in the online environment, seem to opt for a combination of consent and privacy notices and the layered format, whereby the consent banner, containing the most relevant information, constitutes the first layer and the full privacy notice with all other relevant details is linked to as the second layer. The European Data Protection Board seems to support such an approach as they clearly differentiate between the minimum content requirements for the collection of consent and the general compliance with Art. 13 and 14 of the GDPR.[370] In accordance to their Guidelines, the data subject should at least be provided with details regarding the controller's identity; the purpose of processing; the type of data to be processed; the applicability of the individual's right to withdraw consent; where relevant, information about the use of the data for automated decision-making as per Article 22(2)(c) No. 3 and any possible data transfer to third countries, as well as the associated risks to be disclosed to the individual in order for their consent to be qualified as informed.[371] The exact same list has also been previously supported by the Art. 29 WP in their Guidelines on Consent as well.[372]

---

[369] *Lee/Lee*, 21 Psychol. Mark. 2004, 159, 159ff; *Bawden/Holtham/Courtney*, 51 Aslib Proceedings 1999, 249, 249ff; https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1360 (accessed: 05 March 2026).

[370] *EDPB*, Guidelines 05/2020, para 64-65, 72.

[371] *EDPB*, Guidelines 05/2020, para 64.

[372] *Art. 29 WP*, Guidelines on consent, 13.

b) Format

The GDPR does not provide for any general requirements regarding the form in which information is to be provided to the individual. The European Data Protection Board (EDPB) outlines in that context that the way of presentation may include means such as written or oral statements, as well as audio or video messages.[373] From a compliance perspective it should, however, be noted that since Art. 7(1) puts the obligation on the controller to be able to "demonstrate" the valid obtainment of consent, the use of permanent forms which can be used as evidence is most likely advisable.[374] Based on that, oral statements made by the controller should ideally be recorded. Also, since the general requirements of transparency apply here as well, information will need to be presented in a form comprehensible for the data subject.[375] The previously outlined rules with regard to the provision of transparent information, such as the need to refrain from the use of lengthy, excessive notices containing many technical details or legal jargon, will therefore still apply.[376]

Whereas there are no comprehensive global requirements regarding the format, Art. 7(2) does provide for certain formalities, for instance where consent is provided in combination with a written declaration, concerning other matters as well. Should this be the case, the request for consent needs to be presented in a form, which is "clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language". This provision originally has its roots in the German Federal Data Protection Act of 1990, Section 4(a), which required that where consent is given in writing at the same time as other declarations, "special prominence

---

[373] *EDPB*, Guidelines 05/2020, para 66.

[374] Sydow/Marsch / *Ingold*, Art. 7, para 53.

[375] Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 60; *Ernst*, 3 ZD 2017, 110, 113; *EDPB*, Guidelines 05/2020, para 67- 69; LG Frankfurt, DuD 2016, 613, 616.

[376] See Part 1 Chapter 2: B. I. 1. Form.

shall be given to the declaration of consent".[377] The obligation essentially serves the purpose of assuring that controllers do not "hide" privacy relevant information within the general terms and conditions of a contract or service agreement and that the data subject is aware of the fact that they are providing consent for the processing of personal data.[378] This notion is also again supported in Recital 42.[379] With regard to the requirements regarding the use of an intelligible, easily accessible form using clear and plain language, the same considerations already outlined earlier in the context of transparency will largely apply.[380] As for the stipulation of creating a clear distinction between the consent declaration and any other matters, visual effects such as the highlighting, bold underlining, colouring or framing of these elements are regularly advised.[381] Since the notion of a written declaration also extends to the digital environment, specific consideration should be taken in order to assure the clear presentation in such context as well since technical constraints such as small screens, limited space or a general disturbance to the provided service might pose particular challenges for the comprehension of information by the user.[382]

---

[377]Kuner and others / *Kosta*, Art. 7, 345, 349; Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 25; Sydow/Marsch / *Ingold*, Art. 7, para 24.

[378]Kühling/Buchner / *Buchner/Kühling*, Art. 7 DSGVO, para 25; *EDPB*, Guidelines 05/2020, para 67; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 71; *Ernst*, 3 ZD 2017, 110, 113.

[379]*„In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given.".*

[380]See Part 1 Chapter 2: B. I. 1. Form.

[381]Rücker/Kugler, *Dienst*, C. Lawful processing, para 458; Kuner and others / *Kosta*, Art. 7, 345, 350; Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Klein,* 'Art. 7' DSGVO, para 27.

[382]Kuner and others / *Kosta*, Art. 7, 345, 350; *EDPB*, Guidelines 05/2020, para 71. Also, Recital 32 GDPR: "*If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."*

4. Unambiguous

Last but not least, Art. 4 No. 11 provides that consent under the GDPR needs to constitute an "unambiguous indication of the data subject's wishes", through which the individual signifies their agreement with the processing activity through the provision of "a statement or by a clear affirmative action". This means that there should be no doubt as to what the intention of a person's action was and that it must be clear from the overall circumstances that they wished to provide their consent.[383] This criterion was in a sense added to the GDPR, in comparison to the Data Protection directive, as it was not part of the definition of consent under Article 2(h).[384] The requirement of "ambiguity" of consent was, however, included where it constituted a legal basis for the processing of personal data (Art. 7(a) DPD) and when used as a derogation for allowing data transfers to third countries (Art. 26(1) DPD), similar to the now required "explicit" consent under Art. 49(1)(a) GDPR. Still, the actual practical implications of this stipulation were for a long time subject to unclarity,[385] with the German Federal Court of Justice, for example, supporting the possibility of obtaining valid consent through "opt-out" solutions in the rulings on Payback[386] and Happy Digits[387]. The CJEU's ruling in the case of Planet 49 confirmed that, in order to be considered unambiguous, the provision of consent must be related to active behaviour and cannot be collected through pre-ticked checkboxes.[388] The

---

[383]*EDPB*, Guidelines 05/2020, para 75; Rücker/Kugler, *Dienst*, C. Lawful processing, para 455.

[384]See Article 2(h) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: "*'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".

[385]*van Raay/Meyer-van Raay*, 3 VuR 2009, 103, 103ff.

[386]BGH, NJW 2008, 3055, para 23f.

[387]BGH, NJW 2010, 864, para 22f.

[388]Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 54f.

GDPR also further underlined that fact in Recital 32, which lists ticking a box or choosing a technical setting as examples of a clear indication but explicitly excludes silence, pre-ticked boxes, and inactivity from the scope of operations allowing the collection of consent.

Another element requiring consideration in that context is the question of validity of inferred or implied consent. The wording of the GDPR does, at least, not seem to preclude this possibility entirely, since Art. 4 No. 11 does ask for a clear affirmative action signifying agreement but not setting out any formal requirements as to how this would be asserted. Also Recital 32 includes the reference to "another statement or conduct which clearly indicates in this context the data subject's acceptance", also implying that as long as the agreement to the processing activity can clearly be inferred from the overall context, implied consent could be conceivable.[389] This would also be supported by the fact that the criterion of explicitness of consent, which was part of the Commission's proposal, was dropped in the finalised version of the GDPR only making its way into Articles 9(2)(a), 22(2)(c) and 49(1)(a) which concern more sensitive types of processing activities.[390] The European Data Protection Board and the Art. 29 Working Party, however, do not seem to support that notion. Whereas the Working Party's Opinion 15/2011 on the definition of consent under the Data Protection Directive explicitly dealt with this subject, outlining that "unambiguous consent may be inferred from certain actions, in particular this will be the case when the actions lead to an unmistakable conclusion that consent is given",[391] newer Guidelines have completely omitted that part.[392] The prevailing opinion, however, still seems to support the notion of inferring

---

[389]Rücker/Kugler, *Dienst*, C. Lawful processing, para 440f.

[390]*Krohm*, 8 ZD 2016, 368, 371f; Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 185; Rücker/Kugler, *Dienst*, C. Lawful processing, para 440f.

[391]*Art. 29 WP*, Opinion 15/2011, 23.

[392]*EDPB*, Guidelines 05/2020 and *Art. 29 WP*, Guidelines on consent.

consent from a clear action of the individual, indicating their agreement to a specific processing activity.[393] This notion should not be used excessively and would only apply in circumstances where the intention of the individual is clear and the person was able to form an understanding as to the intended processing activity in advance. Also, considering that in accordance with Art. 7(1) GDPR, the controller has the burden of proving the valid obtainment of consent from the data subject, businesses might be hesitant to base processing activities on implied agreement, considering the potential risks.[394] This risk applies even more so when businesses are, for example, entering into a contractual relationship with the individual, as in that case the formal requirements of Art. 7(2) will apply additionally, obliging the controller to clearly differentiate agreement to any additional processing of personal data from any other matters. In that sense, the use of implied consent should most likely be limited to circumstances where no doubt regarding the individual's actions can arise.

Often considered in that context is the use of browser settings for obtaining consent for cookies and other tracking techniques in order to avoid consent fatigue on the side of the data subject.[395] Recital 32 seems to be supportive of that idea, since the possibility of providing consent by "choosing technical settings for information society services" is explicitly mentioned therein. The problem which, however, at this point largely hinders the allowance of cookies through browser settings is the lack of granularity as individuals would not be able to specifically select the purposes for which tracking should be allowed, as well as lack of information since the browser is unlikely to be able to provide the necessary information for each website visited by the

---

[393] *Hacker*, Datenprivatrecht, 165; *Kosta,* Consent*,* 168f; Rücker/Kugler, *Dienst*, C. Lawful processing, para 440f; *Krohm*, 8 ZD 2016, 368, 371f; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 35; *Ernst*, 3 ZD 2017, 110, 114; Wolff/Brink/v. Ungern-Sternberg / *Stemmer*, Art. 7 DSGVO, para 84.

[394] Wolff/Brink/v. Ungern-Sternberg / *Stemmer*, Art. 7 DSGVO, para 84; Rücker/Kugler, *Dienst*, C. Lawful processing, para 440f.

[395] *Loy/Baumgartner*, 8 ZD 2021, 404, 406; *Hanloser*, 8 ZD 2021, 399, 402f; *Sesing*, 7 MMR 2021, 544, 548; *EDPB*, Guidelines 05/2020, para 89.

individual in advance.[396] In light of these issues, Personal Information Management Systems are in fact frequently mentioned as a potential tool to facilitate a more sensible approach towards cookie notices, while at the same time providing for the possibility of obtaining consent in accordance with all the requirements applying to such under the GDPR.[397] The requirement for consent to be unambiguous also further supports the general notion of obtaining consent by technological means, since its obtainment can easily be protocoled and evidenced in that context.[398]

II. Specific Requirements

Whereas the previous section described the requirements for all types of consent provided for the processing of personal data in general, there are also a few areas in which the GDPR introduces additional stipulations or even exemptions in certain contexts. These can either result from the type of processing activities, special characteristics of the parties involved, or the categories of data concerned. In order to provide a full picture on the subject of consent, these will therefore be analysed in further detail.

1. Explicit Consent

Additionally, to the prerequisites of consent to be freely given, specific, informed and unambiguous, the GDPR also introduces the requirement for consent to be "explicit" in three instances. First of all, while the processing of special categories of personal data is in principle prohibited, in accordance with Art. 9(1), Paragraph 2 outlines a

---

[396] https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf (accessed 04 March 2026); *EDPB*, Guidelines 05/2020, para 89; *Loy/Baumgartner*, 8 ZD 2021, 404, 406ff.

[397] *Becker*, 37 CR 2021, 87, 87ff; *Schumacher/Sydow/von Schönfeld*, 8 MMR 2021, 603, 604f; *Hanloser*, 8 ZD 2021, 399, 403; *Sesing*, 7 MMR 2021, 544, 548.

[398] *Sattler*, Informationelle Privatautonomie, 392.

number of exemptions under which such activities would be permissible. In accordance with Art. 9(2)(a), the prohibition does not apply where the data subject "has given explicit consent" to the processing of these data points unless Member State law does not allow for such to be obtained in connection to a specific processing activity. Secondly, whereas Art. 22(1) also establishes a general right for individuals not to be subject to decisions producing legal or similar effects solely based on automated decision making, Paragraph 2 Point (c) therein allows it under the condition of the data subject's explicit consent. The final mention of explicit consent is found in Art. 49, which provides for derogation for specific situations in the context of transfers of personal data to third countries and international organisations. The general rules applicable to such are outlined throughout Chapter V and have the purpose of assuring that an adequate level of protection is being adhered to, where personal data is transmitted into territories in which the GDPR does not apply. This is mostly achieved by means of adequacy decisions (Art. 45) and so called "appropriate safeguards" (Art. 46). Where such means can, however, not be used by the controllers, Art. 49(1)(a) provides that a transfer may still take place where the individual has been informed about the involved risk resulting from the absence of an adequacy decision and appropriate safeguards and in spite of these, has explicitly agreed to the transfer.

These modalities all follow the same general pattern: a processing activity which potentially generates a high risk for the rights and freedoms of the data subject, is in principle prohibited. If, however, the individual, being aware of the risk, still wished to authorise the processing, the activity can take place after all. These, therefore, in a sense constitute a display of the right of self-determination: if a person explicitly wishes to take a risk, they should be free to do so. What is however not entirely clear, is what the formal requirements for the collection of such actually are and how exactly they differ from the already present demand for a "freely given, specific, informed and unambiguous indication of the data subject's wishes" in the context

of "regular" consent. Certainly the previously discussed idea of implied or inferred consent can be ruled out in this context.[399] Most sources also point out that the specific types of risks and data categories should be specifically outlined.[400] There also seems to be general consensus with regards to the fact that a written statement is not formally required, although advisable since the burden of proof in that regard is put on the controller.[401] The EDPB, for example, suggests the implementation of a two-stage verification procedure as a valid alternative to collection of written, express statements of consent.[402]

While the general intention of the lawmakers in including an additional layer of protection to the requirements of consent for processing operations which are particularly risky is understandable, considering the already applicable conditions, the addition of the prerequisite for consent to be "explicit" seems to be of limited practical relevance. The need for a clear statement which is not hidden in a wall of text with the general terms and conditions or in fine print, already results from the demand for "unambiguous" indication of the data subject's wishes. The demand for the specific risk or categories of data to be explicitly outlined could also arguably have been inferred from the necessity for such to be "informed" and granular. Also, the fact that certain high-risk processing activities require a higher threshold of care and that making sure all necessary elements for valid consent to apply would be investigated more stringently in such contexts, naturally results from the general risk-based approach laid down in the GDPR. In that sense, other than the fact that

---

[399] Ehmann/Selmayr, *Schiff*, Art. 9, para 34; *Krohm*, 8 ZD 2016, 368, 371; Rücker/Kugler, *Dienst*, C. Lawful processing, para 485; Kuner and others / *Georgieva/Kuner*, Art. 9, 365, 377; Kuner and others / *Kuner*, Art. 49, 841, 847.

[400] *Spindler/Dalby* / Spindler/Schuster, Art. 9 DS-GVO, para 23; Kuner and others / *Kuner*, Art. 49, 841, 847; Rücker/Kugler, *Dienst*, C. Lawful processing, para 485.

[401] Gola/Heckmann / *Schulz*, Art. 9 DSGVO, para 24; Wolff/Brink/v. Ungern-Sternberg / *Stemmer*, Art. 7 DSGVO, para 83; *EDPB*, Guidelines 05/2020, para 94.

[402] *EDPB*, Guidelines 05/2020, para 98.

consent notices will not at times include the wording "I explicitly consent" or have an additional check-box, the actual level of protection for the individual's personal data added by this stipulation seems to be purely theoretical.

2. Information Society Services offered to Children

Another area where additional stipulations for obtaining consent for the processing of personal data are introduced refers to the information society service offered to children. This is based on the consideration that children constitute an especially vulnerable group of data subjects and to that extent, require additional protection.[403] In that respect, Recital 38 explains that individuals below a certain age may be less aware of the risk, consequences and safeguards relating to the processing of personal data, as well as their rights related to such. Due to that fact Art. 8(1) provides that in principle, valid consent cannot be obtained from individuals below the age of 16 unless Member State Law provides for a lower age limit which can, however, also not be set below 13. In circumstances where the data subject has not yet reached the required age, consent needs to be given or authorised by the holder of parental responsibility.

a) Applicability

The term "Information Society Services" has already been defined in Art. 4 No. 25 by referring to the definition contained in Art. 1(1)(b) of Directive (EU) 2015/1535, wherein these are described as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". The term "at a distance" refers to instances where the parties are not simultaneously present, whereas electronic means cover any services which are sent initially and received through electronic equipment or other electromagnetic means. In that sense, offerings where

---

[403] Kuner and others / *Kosta*, Art. 8, 355, 356; *EDPB*, Guidelines 05/2020, para 124; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 2.

goods or services are being ordered over the internet and subsequently delivered or provided at the data subject's residence or in another in-person format, would not be included.[404] The same pertains to elements such as phone consultations or online ticket bookings.[405]

Recital 38 also outlines that parental consent should not be required where services are provided in the context of "preventive or counselling services offered directly to a child". Naturally it makes sense to exclude the legal guardians from involvement in these instances in order to assure confidentiality for the child, as they might be reprehensible to share their problems with such, especially where potential conflicts might in fact concern them.[406] The introduction of this exemption is, however, in a sense problematic since Art. 8 does not introduce any differentiation in connection to the type of information society services offered or their purpose.[407] The considerations therein could therefore generally be read as an indication that these types of services will largely not fall under the definition of Art. 8.[408] First, any sort of consultation over the phone will be included in the term of information society services.[409] Second, these types of services would typically be provided, free of charge and as far as possible, without the capturing of personal data.[410] Also, where personal data would need to be processed, other legal bases for this

---

[404]Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 13; BGH, NJW 2014, 2282.

[405]Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 13; Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 144.

[406]*Krivokapić/Adamović*, 64 BLR 2016, 205, 212f; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 8, para 25; *EDPB*, Guidelines 05/2020, para 150.

[407]Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Hilgert,* 'Art. 8' DSGVO, para 22; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 14.

[408]Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 17.

[409]Paal/Pauly / *Frenzel*, Art. 8 DSGVO, para 7; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 17.

[410]Ehmann/Selmayr, *Heckmann/Pascke*, Art. 8, para 25; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 17.

activity are more likely to be used, such as Art. 6(1)(e).[411] In that sense, this dilemma has not yet managed to gain much practical significance. Considering the importance of the subject and the potential risks involved for minors, a direct acknowledgment of this exemption under Art. 8 would have been welcome.[412]

Furthermore, it needs to be considered that the stipulations of Art. 8 do not apply to any service offering of that type but solely to those offered directly to children. In that sense, services which are clearly and openly only intended for the use of adults will be excluded from these obligations.[413] Instances of clear exclusion of certain age groups are, however, likely to be limited and between services which are obviously marketed towards children, such as Cartoon Networks "Free Games for Kids"[414] or You Tube Kids,[415] while those clearly not allowing their use by such lies an extensive variation of so called "dual use" offerings, intended for both audiences.[416] Where children are at least also included within the target group for such offerings, the additional requirements should also apply, since Art. 8 does not ask for an exclusiveness.[417] Should the target group not be clearly defined, all types of elements could be taken into consideration in order to determine if children are also considered as potential con-

---

[411] Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 17.

[412] *Krivokapić/Adamović*, 64 BLR 2016, 205, 212f.

[413] Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 17; Paal/Pauly / *Frenzel*, Art. 8 DSGVO, para 7; *Buchner/Kühling*, 41 DuD 2017, 544, 547; *EDPB*, Guidelines 05/2020, para 130.

[414] https://www.cartoonnetworkhq.com/games (accessed: 23 October 2025).

[415] https://www.youtubekids.com/ (accessed: 23 October 2025).

[416] *Lievens/Verdoodt*, 34 CLSR 2018, 269, 272; *Jandt/Roßnagel*, 10 MMR 2011, 637, 637f; Paal/Pauly / *Frenzel*, Art. 8 DSGVO, para 7; *Buchner/Kühling*, 41 DuD 2017, 544, 547; Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Hilgert,* 'Art. 8' DSGVO, para 29-32.

[417] *Lievens/Verdoodt*, 34 CLSR 2018, 269, 272; *Jandt/Roßnagel*, 10 MMR 2011, 637, 637f; Paal/Pauly / *Frenzel*, Art. 8 DSGVO, para 7; *Buchner/Kühling*, 41 DuD 2017, 544, 547; Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Hilgert,* 'Art. 8' DSGVO, para 29-32.

sumers, such as the content of a service, visuals or the used language.[418] Where, on the other hand, a certain good or service is intended for use by children but it is clear that it will not be procured directly by them (for example because it is clearly marketed towards parents, as something they could purchase for their children) these will not fall under the scope of Art. 8.[419]

b) Verification

Once it has been determined that the criteria for the applicability of Art. 8 are in fact met, the question arises how to practicably verify the individual's age, as well as the presence of parental consent or authorisation, where necessary. The differentiation between parental consent and authorisation is decided based on the fact whether the data subject has provided their consent first.[420] From a practical perspective, the child will either way usually be the first in contact with the provider, since the service is being offered directly to them. In that sense, the difference is largely irrelevant from a practical perspective which is why the two are often referred to interchangeably.[421] Any sort of actual distinction between the two modalities is only likely to appear at the point where the data subject wished for the processing activity to be ceased.[422] The amount of detailed practical guidance available with regard to the verification of these aspects is shockingly low, with most sources simply referring to the consideration of the circumstances and to the applicability of a proportionate or risk-based approach, which would factor in the catego-

---

[418]Rücker/Kugler, *Dienst*, C. Lawful processing, para 463; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 8, para 22.

[419]*Gola/Schulz*, 10 ZD 2013, 475, 478; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 18.

[420]Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 20f.

[421]*EDPB*, Guidelines 05/2020, para 137-151; Kuner and others / *Kosta*, Art. 8, 355, 361f.

[422]*Taeger*, 9 ZD 2021, 505, 508; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 8, para 28-32.

ries of data processed, the average age of users, the type of processing activity and its purposes, as well as the potential risks that might result for the rights and freedoms of the individual as a consequence.[423]

Another problem is that where explicit advice is in fact provided, the actual effectiveness of the suggested measures can be described as questionable at best. Using the example of an online gaming platform, the European Data Protection Board suggests a procedure in which the user is asked to provide their age as a first step and should such lie below the applicable age of consent, be required to enter the e-mail address of their legal guardian who would then be able to provide or decline their authorisation through a link.[424] The use of this or similar forms of double-opt-in procedures where the data subject is asked for the contact details (mostly e-mail addresses) of the holder of parental responsibility, is also largely recommended in the prevailing literature.[425] The potential risks of such a procedure should, however, be quite clear, as there are practically no means to verify if the age declared by the individual is in fact correct or if the legal guardians are actually the ones agreeing via the double-opt-in procedure, since children could either access their parents e-mail address or simply provide one created and controlled by themselves.[426] Still, the prevailing opinion supports the notion that these risks are acceptable and this solution is at the moment to be

---

[423] *EDPB*, Guidelines 05/2020, para 132-137; Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Hilgert,* 'Art. 8' DSGVO, para 47-54; Paal/Pauly / *Frenzel*, Art. 8 DSGVO, para 13; Kuner and others / *Kosta*, Art. 8, 355, 360f.

[424] *EDPB*, Guidelines 05/2020, para 138-142.

[425] *Möhrke-Sobolewski/Klas*, 12 K&R 2016, 373, 377f; *Buchner/Kühling*, 41 DuD 2017, 544, 547; *Gola/Schulz*, 10 ZD 2013, 475, 479; *Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio*, 'Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten', 43; Rücker/Kugler, *Dienst*, C. Lawful processing, para 468.

[426] *Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio*, 'Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten', 43; *Möhrke-Sobolewski/Klas*, 12 K&R 2016, 373, 378; *Gola/Schulz*, 10 ZD 2013, 475, 480.

considered the most constructive one, at least for most types of processing activities.[427]

Such an approach, while perhaps reasonable a few decades ago, seems to lose its ground with each year where children effectively possess more knowledge as to the working of these mechanisms than their parents. In that sense, the whole purpose of protecting vulnerable individuals is at risk of getting lost. Alternative solutions should therefore be explored and developed, if the purpose of Art. 8 is not to be completely undermined. With regards to the topic of age verification, there are in fact already a number of established solutions in the context of online-gambling and the sale of age restricted goods, such as tobacco or alcohol.[428] The significant problems with deploying those analogously in the context of age verification under the GDPR, lies in the underlying age requirement. Offering of goods and services prohibited for minors, coincide with the legally relevant age of majority. Due to that, they can use verification methods, such as IDs, social security numbers, passports or bank account details, which are only issued for adults. The same does not, however, apply in the case of information society services offered to children, which use the age threshold of 16 or lower based on national derogations.[429] Other more advanced and reliable methods include such solutions as offline verification, the adoption of eID cards and the use of biometric data, such as fingerprints or iris patterns.[430] At the current stage, these solutions are, however, mostly disregarded either based on their high level of complexity or ethical and privacy concerns, based on the use of an excessive amount of additional (sensitive) personal data.[431] While the GDPR does not explicitly state that

---

[427] ibid.

[428] *Nash and others*, Effective Age Verification, 25-30; https://s3.eu-west-2.amazonaws.com/sr-acuk-craft/documents/Effective-age-gating-for-online-alcohol-sales-Final-Report.pdf (accessed: 26 February 2026) 9-16.

[429] *Macenaite/Kosta*, 26 Inf. Commun. Technol. Law. 2017, 146, 180.

[430] ibid 181.

[431] *Macenaite/Kosta*, 26 Inf. Commun. Technol. Law. 2017, 146, 181; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 26; *Möhrke-Sobolewski/Klas*, 12 K&R 2016, 373, 377; Rücker/Kugler, *Dienst*, C. Lawful processing, para 469.

the measures for age verification adopted by the controller would need to be "reasonable" as has been with regards to the confirmation of parental consent, it is generally considered that the efforts taken by the controller in that context should be selected in consideration of their reasonableness and proportionality.[432]

A look across the Atlantic might be beneficial in the context of verifying the data subject's age, as well as parental consent and/or authorisation, using the experience as well as techniques developed and discussed in the context of the requirements of the Children's Online Privacy Protection Act (COPPA).[433] Here operators of websites or online services directed at children have been subject to similar obligations for over two decades and accordingly, have attempted to strike a balance between effective verification methods and the possibilities of their practical implementation.[434] While the implemented age verification mechanisms, which also rely on the user's self-assertion, have been subject to substantive criticism based on their ineffectiveness,[435] a number of interesting solutions have been developed with regards to the collection of parental consent.[436] The Federal Trade Commission has, for example, approved the following methods: (1) print-and-send, whereby a consent form signed by the parent needs to be returned via mail, fax or electronic scan; (2) requiring the use of a parent's credit card or other form of online payment, which assures that the account holder is notified regarding such; (3) asking the parent to call a phone number or attend a video conference with trained personnel; (4) verification of the parents' identity through cross-reference with governmental databases;

---

[432] *Taeger*, 9 ZD 2021, 505, 507; *EDPB*, Guidelines 05/2020, para 132f; Kuner and others / *Kosta*, Art. 8, 355, 360; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 8, para 29.

[433] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

[434] For a comparison between the two regulatory systems, as well as an overview of used measures refer to: *Rauda,* 1 MMR 2017, 15, 15ff.

[435] *Hoofnagle*, FTC Privacy Law and Policy, 109.

[436] *Macenaite/Kosta*, 26 Inf. Commun. Technol. Law. 2017, 146, 168f; *Buchner/Kühling*, 41 DuD 2017, 544, 547; Kühling/Buchner / *Buchner/Kühling*, Art. 8 DSGVO, para 25.

(5) asking a number of questions which would be difficult to answer for an individual below a certain age; or (6) verification of a photo on the parents driver's license or ID, against a provided picture, through the use of facial recognition technology.[437] While some of these might be disproportionate in consideration of the processing activity at question,[438] the possibilities of deploying alternative and most importantly more effective mechanisms should be examined. Especially the idea of conducting a short phone call or a video conference seems to be a reasonable solution, through which at least individuals significantly below the required age restriction could be identified. After all, there are already multiple service providers specialised in online identification procedures on the market.[439] While they are currently predominantly used in context such as opening online bank accounts or brokerage services, there is no reason why they should not be extended to the sphere of online age verification.

c) Adpotion by PIMS

The considerations of new solutions could therefore be quite interesting in the context of offering Personal Information Management Systems. This will not only be the case due to the current lacking on the market but also since those arguably have a bigger potential, with regards to the proportionality of such measures, than regular controller–data subject relationships. As outlined previously, both the alternative methods for confirming parental consent supported by the

---

[437]See: FTC, 'Complying with COPPA: Frequently Asked Questions', https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#_blank (accessed: 15 April 2026).

[438]For example, if facial recognition technology was to be used for the verification of consent in the case of an online game, not collecting any significant amount of personal data in the first place.

[439]See for example: PostIdent, https://www.deutschepost.de/de/p/postident.html (accessed 22 October 2025); E-Verify, https://www.e-verify.gov/ (accessed: 22 October 2025); Seon; https://seon.io/resources/what-is-identity-verification/ (accessed 22 October 2025); IDNow, https://www.idnow.io/products/idnow-videoident/ (accessed 22 October 2025).

FTC, as well as many other proposals made over the years with regard to age verification, are largely disregarded based on considerations of proportionality of such measures. These arguments are mostly based on the fact that processes which truly guarantee the authenticity of validation require the implementation of such extensive processing operations and the use of a large amount of additional personal data, making them excessive in comparison to the underlying processing activity. Another argument often pertains to the fact that these procedures call for an immense amount of resources, on the side of the controller, thereby making them "unreasonable".

Both of these points of contention can, however, reach a significantly different outcome in the context of PIMS. First, a consent management platform will generally administer user preferences across multiple platforms. In that sense, while a certain mechanism might have been designated as "excessive" for a specific processing activity, the assessment of proportionality might reach a different outcome if the same procedure is being used for various processing activities at once, especially if some of those are in fact high risk. In that sense, lower risk processing might actually benefit from high-risk activities. Also, since the platform would only require such a complex form of verification to be conducted once, the burden put on the individual would also be significantly lower. Last but not least, the goalpost of what is to be considered "reasonable" would also be considerably moved. In the case of typical controllers, the processing of personal data will mostly constitute a side effect of the actions performed in order to achieve the goals of the underlying business model. In that sense, especially with verification mechanisms requiring a large amount of resources, the conclusion can be reached that such are "unreasonable". With PIMS, however, the entire underlying business model lies precisely in the assurance of the individual's rights and in the processing of their personal data. In that sense, the deployment of high-level, resource intensive, state-of-the-art solutions can no longer be regarded as excessive but should rather be considered as a reasonable expectation on the side of the consumer.

3. Scientific Research

Processing of personal data for the purposes of archiving in the public interest, statistic and scientific or historical research are to a certain extent privileged under the GDPR.[440] This is evidenced through the multitude special rules, as well as the permission for derogations to be introduced by the Member States, provided throughout the text of Regulation.[441] These rules, allowing to a certain extent for a higher degree of flexibility are based on the assumption that scientific research aims to grow the collective knowledge, as well as well-being of society.[442] In the context of consent, these are mainly demonstrated through the introduction of the concept of broad consent and the provision of an additional legal basis for the processing of sensitive personal data.

a) Broad Consent

The notion of broad has been outlined in Recital 33, which states that it should be possible for data subjects to provide their consent for certain areas of scientific research in general, rather than for a specific pre-defined purpose, as would normally be required under the stipulation of "specific" consent. The rule is based on the consideration that a thorough and detailed definition of the purposes of a research project will often not be entirely possible, as further steps are frequently based on conclusions reached within the first phases of such or since it is possible to discover findings and connection which could not have been foreseen.[443] This is especially relevant in

---

[440] *Chico*, 128 Br. Med. Bull. 2018, 109, 110; *Becker and others*, 30 EJHL 2023, 129, 145-151; *Rossnagel*, 4 ZD 2019, 157, 159; *Weichert*, 1 ZD 2020, 18, 18ff; *Johannes/Richter*, 41 DuD 2017, 300, 300ff.

[441] See for example: Art. 5(1)(b) and (e), Art. 9(2)(j); Art. 14(5)(b), Art. 17(3)(d), Art. 21(6) and Art. 89, as well as Recitals 33, 50, 52, 53, 62, 65, 113, 156, 157, 159, 161 and 162.

[442] *EDPS*, Preliminary Opinion, 2.

[443] Ehmann/Selmayr, *Raum*, Art. 89, para 37; *EDPB*, Guidelines 05/2020, para 156.

the context of long-term studies, as well as large data repositories such as Biobanks.[444]

This notion, however, does not mean that the general requirements for consent are to be completely disregarded. First, the general aims of the project as well as envisaged consequences should still be laid down in as much detail as possible and all areas for uncertainty should be also be transparently presented as such, including the reasons for the current unpredictability of certain processes and/or outcomes.[445] Also, in line with the notion of granularity of consent (see Part 1 Chapter 2: C. I. 1. c) Granularity), to the extent that this is possible in consideration of the research project at hand, individuals should be given the option to solely provide their consent for certain areas of research or parts of a specific project.[446] Another relevant consideration in that context relates to the previously mentioned requirements regarding the format of providing the relevant information. As outlined under Part 1 Chapter 2: C. I. 3. b) Format Article 7(2) provides that where consent for the processing of personal data is collected in combination with other written declarations, it needs to be clearly distinguishable from such. Considering the extensive amount of information usually provided to participants of research projects, it is therefore crucial to clearly separate the consent form for the processing of personal data from the rest of the documentation. The EDPB further highlights the necessity of that differentiation by noting that the consent for the use of personal data has to be "distinguished from other consent requirements that serve as an ethical standard or procedural obligation".[447] This means that the individual's consent for participating in a research project and the

---

[444] *Rossnagel*, 4 ZD 2019, 157, 160; Ehmann/Selmayr, *Raum*, Art. 89, para 37; *Schaar*, 5 ZD 2017, 213, 214; *Hänold*, 1 ZD-Aktuell 2021, 05016; *Hänold*, 2 ZD-Aktuell 2020, 06954.

[445] *EDPB*, Guidelines 05/2020, para 161f; *EDPB,* clarifications on health research, para 27.

[446]; *EDPB,* clarifications on health research, para 26; *Schaar*, 5 ZD 2017, 213, 215.

[447] *EDPB*, Guidelines 05/2020, para 154.

agreement to the processing of personal data required for such would effectively need to be collected separately.[448] Last but not least, Recital 33 sets out the obligation for recognised ethical standards for scientific research to be kept, in order for the notion of "broad consent" to apply. Since the requirements applicable in that area are both numerous and extensive,[449] comprehensive guarantees for the assurance of the rights of the individual will already be in place based on those.

b) Dynamic Consent

Another special form of consent often considered and discussed in the context of scientific and especially biomedical research is the concept of "dynamic consent".[450] Behind this concept lies the idea that instead of providing data subjects with generalised (mostly paper-based) consent forms and requesting them to allow the processing of their personal data, ongoing communication between researchers and the participants should be facilitated.[451] Since researchers are often unable to foresee how the data might be used in subsequent stages of the project, this would allow individuals to receive updates regarding the following steps, findings and continuation, including the underlying processing activity.[452] Individuals would then have the option to check and revise the authorisation provided by them over time.[453] The deployment of such platforms therefore

---

[448]Research Projects should therefore carefully consider whether or not consent should in fact be used as the legal basis for processing personal data, or to what extent one of the other legal bases found in Art. 6 could apply.

[449]See for example: *ALLEA*, 'The European Code of Conduct for Research Integrity'; *WHO*, 'CoC for Research'; *European Commission*, Ethics and data protection (14 November 2018).

[450]*Prictor and others*, 3 JDPP 2019, 93, 93 ff**;** Ehmann/Selmayr, *Raum*, Art. 89, para 38; *Kaye and others*, 23 Eur J Hum Genet 2015. 141, 141-146; *Teare/Prictor/Kaye*, 29 Eur J Hum Genet 2021, 649, 649ff; *Albanese/Calbimonte/Schumacher,/Calvaresi*, 11 J Ambient Intell Human Comput 2020, 4909, 4909 ff.

[451]*Kaye and others*, 23 Eur J Hum Genet 2015. 141, 141.

[452]ibid.

[453]*Teare/Prictor/Kaye*, 29 Eur J Hum Genet 2021, 649, 649.

solves the inherent problems with the inability to provide sufficiently precise information at the beginning of a research project, and allows for all the requirements of consent to be adopted accordingly, including the ability to withdraw such at any given time, without hindrance.

aa) Capabilities and Drawbacks

Due to this clear potential in solving the inherent problems of assuring that data is in fact processed in accordance with the individual's wishes, as well as the substantial interest of researchers to assure the continuous availability of such datasets and allow access for new purposes, numerous initiatives supporting this notion have developed over the years. Examples include platforms such as Dwarna,[454] ScoDES,[455] ConsentChain,[456] or RUDY,[457] just to name a few. While all of these deploy varying IT infrastructures, as well as modalities in the means of communication with the data subject, they effectively follow the same goal and attempt to solve similar issues such as enabling personalised communication, improving transparency and scientific literacy, streamlining recruitment, and allowing fine grained withdrawal.[458] The idea of deploying such dynamic consent platforms in the context of scientific research is, however, not without its detractors. Arguments brought against these often refer to the fact that these solutions require a large amount of resources, making them widely impractical.[459] Fears are also voiced that participants might in fact be overwhelmed by the level of detail and complexity of the provided information, potentially leading to feelings of incompetence and insecurity regarding their own decisions[460] and

---

[454] *Mamo/Martin/Desira/Ellul/Ebejer*, 28 Eur J Hum Genet 2020, 609, 609ff.

[455] *Albanese/Calbimonte/Schumacher,/Calvaresi*, 11 J Ambient Intell Human Comput 2020, 4909, 4909ff.

[456] *Albalwy/Brass/Davies,* 9 JMIR 2021, e27816.

[457] *Teare and others*, 25 Eur J Hum Genet 2017, 816, 816ff.

[458] *Kaye and others*, 23 Eur J Hum Genet 2015. 141, 143ff; *Teare/Prictor/Kaye*, 29 Eur J Hum Genet 2021, 649, 651.

[459] *Hänold*, 2 ZD-Aktuell 2020, 06954; *Teare/Prictor/Kaye*, 29 Eur J Hum Genet 2021, 649, 650.

[460] *Steinsbekk/Myskja/Solberg*, 21 Eur J Hum Genet 2013, 897, 899.

that such a close relationship creates an unrealistic expectation as to the actual outcome of a project or may invoke a desire for reciprocity[461].

bb) Dynamic Consent and PIMS

Regardless of the potential issues and obstacles resulting from the use of consent platforms in the context of scientific research, one point should be abundantly clear: the aim of these platforms is directed toward enabling research participants to take active control over the processing of their (personal) data. Based on that, they must definitely be considered Personal Information Management Systems in accordance with the leading definition. It is surprising in that context that none of the mentioned projects, nor any other related to the management of individual's consent for the participating in scientific research, have been mentioned in the publications surrounding the subject of PIMS. The focus of such seems to be largely on commercial tools and projects working on the management of consent in the online context, such as social media, user accounts or cookies.[462] The European Data Protection Supervisor (EDPS), on the other hand, does refer to the use of PIMS for effective consent management in the field of research but solely mentions that it *"could be explored whether it can make sense, and under what safeguards and conditions, to express consent for broader, wider contexts such as medical research sectors"*,[463] completely ignoring the already existing substantive projects and developments in that area.

This does inadvertently raise the question whether platforms run for these purposes are generally excluded from the definition of PIMS. Such a conclusion would, however, make little sense, considering that the EDPS does mention the possibility of exploring these

---

[461] *Levitt*, 19 Health Care Anal 2011, 220, 220 ff.

[462] *Jentzsch*, Datenökonomie, 36f; *European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016), 5f; *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 6-8; *Attoresi/Moraes*, TechDispatch #3/2020, 1.

[463] *EDPS*, Opinion 9/2016, para 25.

modalities in the context of medical research. Also, certain platforms do include the option for users to sell or donate their personal data for research purposes[464] While these are presumably mostly used for the implementation of commercial market research rather than scientific or historical purposes and will not be conducted for the "public interest", meaning that they would not be able to benefit from the privileged status granted to such by the GDPR,[465] it shows that PIMS are in fact used for the facilitation of research (in a general meaning) as well. In that sense, dynamic consent platforms run for research purposes should be considered a special category of Personal Information Management Systems. On the one hand, the burdens for running such systems will be significantly higher, considering the numerous and extensive ethical standards applicable in that area, as well as the requirement to distinguish the general consent for participation in a research project, from the authorisation to process one's personal data. On the other hand, especially when it comes to the idea of the ethical treatment of data, and the involvement of individuals and transparent provision of information, all areas of research from clinical trials to social studies, have a vast amount of experience which could and should be used by developers of Personal Information Management Systems.

cc) Explicit Consent

As outlined previously (see Part 1 Chapter 2: C. II. 1. Explicit Consent), Article 9(2)(a) introduces the additional requirement for consent to be "explicit" in instances where it concerns the processing of special categories of personal data. This is in fact quite relevant in the area of scientific research, where information concerning the in-

---

[464] https://www.dailymail.co.uk/sciencetech/article-6653517/Firm-launches-ethical-data-platform-users-sell-data.html (accessed: 25 February 2026).

[465] *Hornung/Hofmann*, 4 ZD-Beilage 2017, 1, 4-9; Ehmann/Selmayr, *Schiff*, Art. 9, para 64.

dividual's health, as well as genetic or biometric data, is in fact frequently subject to processing.[466] It should therefore be mentioned that Art. 9(2)(j) also provides for an alternative legal basis for such as it stipulates that based on Union or Member State law, it can also set out specific derogations, allowing the processing of such data points in accordance with Art. 89(1), where it is necessary for archiving in the public interest, scientific or historical research purposes or statistical purposes. While this does not constitute a form of exemption in the context of the general consent requirements, it does provide controllers with a certain amount of flexibility as to which legal basis to select where a derogation is in fact applicable.[467]

Where obtaining the management of GDPR compliant consent, as well as all legal stipulations accompanied by such (for example the right to withdrawal) would be too burdensome for a project or in fact hinder its execution, the use of such an alternative legal basis might be quite useful. On the other hand, this should not be mistaken for a general relief as the use of this legal basis naturally comes with its own set of additional requirements itself. In particular, assurance of measures protecting the rights and interest of the individual, as well as the respect for the essence of the right, need to be considered and "appropriate safeguards" in the meaning of Art. 89(1) put in place.[468] Also, the consent of the individual to participate in the research project in general will most likely still have to be obtained based on ethical requirements applicable in the field.[469] In that sense, the use of another legal basis is likely to lead to the quite confusing outcome in which consent is obtained but not used as the basis for processing personal data. In that sense, controllers will have to de-

---

[466] *Rossnagel*, 4 ZD 2019, 157, 161; *Nordberg*, in: GDPR and Biobanking, 61, 72-74; Kuner and others / *Georgieva/Kuner*, Art. 9, 365, 373-375.

[467] *Cepic*, 10 ZD-Aktuell 2021, 05214; *Rossnagel*, 4 ZD 2019, 157, 161.

[468] *Kipker/Schaar*, 15 ZD-Aktuell 2017, 04263; Kuner and others / *Georgieva/Kuner*, Art. 9, 365, 380f.

[469] *EDPB,* clarifications on health research, para 7.

termine on a case-by-case basis, considering the overall circumstances of the research project, to what extent circumventing Art. 9(2)(a) is in their and the data subject's best interest.[470]

III. Behavioural Obstacles

The previous section focused on the formal legal requirements connected to the use of consent as a legal basis for processing personal data. Here a number of challenges with the collection of valid consent have already been identified such as the imbalance of powers between the parties, conditionality, granularity, the provision of transparent information, and distinguishing consent from other matters, as well as making sure that consent is in fact provided for a specific processing activity and not in a too generalised form. There are, however, also a number of hindrances relating more to the social and behavioural aspect of how decisions are effectively made by individuals which also call into question the validity of certain authorisations and have led to extensive criticism of this legal basis within literature. [471]

This closely relates to the so called “privacy paradox” which describes to the common observation especially in the context of user online behaviour, that while individuals typically report a strong concern for the protection of their personal data, they paradoxically still frequently engage in behaviour which severely compromises their privacy.[472] Privacy professionals, advocates and experts from the

---

[470]For more considerations on this subject refer to: *Chen/Dove/Bhakuni*, in: Research Handbook, 474, 474ff.

[471]*Kamp/Rost*, 37 DuD 2013, 80, 80-83; *Hacker*, Datenprivatrecht, 255-258; *Efroni and others*, 5 EDPL 2019, 352, 355-357; *Blume*, 2 IDPL 2012, 26, 29; *Calo*, 87 Notre Dame Law Rev. 2013, 1027, 1050ff; *Hermstrüwer*, Selbstgefährdung, 227ff; *Koops*, 4 IDPL 2014, 250, 251ff.

[472]*Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 211; *Gerber/Gerber/Volkamer*, 77 Comput. Secur. 2018, 226, 226ff, *Barth and others*, 41 TELEMAT INFORM 2019, 55, 55ff; *Baek*, 38 CHB 2014, 33, 33ff; *Acquisti/Grossklags*, 3 IEEE Security & Privacy 2005, 26, 26ff; *Hermstrüwer*, 8 JIPITEC 2017, 9, para 29.

fields of law, social, behavioural, and economic studies have therefore researched this phenomenon and come to varying conclusions and theories regarding its origins. While a regret on the users' side concerning their decision or miscommunication of a preference does not automatically lead to a legal invalidation of the collected consent on the side of the controller, it does in a sense constitute a hindrance in the effective execution of the data subject's actual wishes, as well as the exercise of their right to self-determination. These obstacles are also, to a large extent, the motivation behind the development of new privacy enhancing technologies attempting to mitigate the identified issue. Since they have been discussed at length within privacy related literature, the following section will only provide a general overview, rather than a deep dive into the subject matter.

1. Bounded Rationality

The term "bounded rationality" refers to the restriction when it comes to rational human decision-making, which inevitably results from the cognitive limitations of the decision-maker, both in the context of knowledge and computational capacity.[473] These can stem from various aspects. What generally comes to mind first in the context of data privacy and informed decision-making, are the already extensively discussed issues regarding the provision of transparent information, inevitably leading to an inability of the data subject to effectively comprehend what the underlying processing activity entails and what the potential consequences might be.[474] Further aggravating this fact are frequently basic constraints of time, limiting the individual's ability to make a truly informed choice, even where theo-

---

[473] *Simon*, in: Utility and Probability, 15-18, *Sent*, 25 EJHET 2018, 1370, 1370ff.

[474] See Part 1 Chapter 2: B. II. Obstacles. Also: *Acquisti/Grossklags*, in: Econ. of Inf. Sec., 165, 165ff; *Reidenberg and others*, 30 BTLJ 2015, 39, 39ff; *Acquisti/Grossklags*, 3 IEEE Security & Privacy 2005, 26, 30f; *Barth and others*, 41 TELEMAT INFORM 2019, 55, 58.

retically they would have been able to process all the relevant factors.[475] A 2008 study concluded that users would need to spend approximately 201 hours on reading privacy policies alone if they were to actually review the complete content.[476] While these are only estimates it is no secret that privacy policies are notoriously long and rarely read, and the GDPR surely did not help alleviate this fact. Due to their excessive length, users are therefore frequently forced to simply "skim" the policies for elements generally relevant for them without considering other factors.[477] In turn, even privacy conscious individuals will be limited in their ability to make a truly informed and rational decision. This problem is even further aggravated where a person may not possess the underlying knowledge to understand the actual processing operations or the resulting risks.

2. Heuristics

These constraints within the individual's capacity to form a truly informed and rational decision lead to the reliance on heuristics, which are mental shortcuts applied in order to ease the cognitive overload of the determination process.[478] The idea that individuals use such simplifications in order to reduce the complexity of an assessment requiring the consideration of various values and probabilities, was introduced by researchers in the 1970's.[479] Whereas the reliance on previous experiences and internalised general rules in the decision-making process is both logical and useful, it does also bear the potential of leading to severe and systematic errors.[480]

---

[475] *Barth and others*, 41 TELEMAT INFORM 2019, 55, 56 and 58; *McDonald/Cranor*, 4 J.L. & Pol'y for Info. Soc'y 2008, 543, 549; *Giese/Stabauer*, in: HCI in Bus., Gov. and Org., 272, 272.

[476] *McDonald/Cranor*, 4 J.L. & Pol'y for Info. Soc'y 2008, 543, 565.

[477] *McDonald/Cranor*, 4 J.L. & Pol'y for Info. Soc'y 2008, 543, 555.

[478] *Hermstrüwer*, 8 JIPITEC 2017, 9, para 33; *Knauff*, in: Rationale Entscheidungen, 15, 15; *Beck*, Behavioral Economics, 25f.

[479] *Tversky/Kahneman*, 80 Psychological Review 1973, 237, 237ff.

[480] *Tversky/Kahneman*, 185 Science 1974, 1124, 1124.

These potential mistakes in judgements also significantly affect the sphere of consent for the processing of personal data, which is why the most commonly identified heuristics of (a) Representativeness, (b) Availability, and (c) Anchoring are analysed below.

a) Representativness

The heuristic of representativeness is typically applied when making a judgement about the probability of something (e.g., What is the probability that object A belongs to class B? What is the probability that event A originates from process B? What is the probability that process R will generate event A?).[481] This judgement is then made based on how well the two elements resemble the class they represent.[482] While the application of this shortcut can in principle lead to quite accurate results, it also typically tends to cause the neglect of other relevant factors such as the prior probability of outcomes (also known as the base-rate-fallacy), sample sizes, and predictability.[483] It also frequently induces illusions of validity, as well as misconceptions of outcome and regression.[484]

In the context of data privacy, the impact of representativeness has, for example, been observed in assessments of the effect of certain vendor characteristics on online user behaviour. A study conducted in 2006 found that while the company's perceived reputation had significant influence on the level of trust reported by consumers, the presence of privacy assurance mechanisms such as policies and seals, barely did.[485] The same tendency was also confirmed in a 2012 report based on 48 semi-structured interviews on the subject of online behavioural advertising, which concluded that participants

---

[481] *Tversky/Kahneman*, 185 Science 1974, 1124, 1124.

[482] *Camerer/Loewenstein*, in: Advances in Behavioral Economics, 3, 10; *Beck*, Behavioral Economics, 28.

[483] *Beck*, Behavioral Economics, 29-38; *Tversky/Kahneman*, 185 Science 1974, 1124, 1124ff; *Tversky/Kahneman*, 80 Psychological Review 1973, 237, 237ff.

[484] *Beck*, Behavioral Economics, 29-38; *Tversky/Kahneman*, 185 Science 1974, 1124, 1124ff; *Tversky/Kahneman*, 80 Psychological Review 1973, 237, 237ff.

[485] *Metzger,* 33 Commun. Res. 2006, 155, 155ff.

would make judgements regarding an entity's privacy practices based on the name of such itself, rather than the actual disclosed processing activities.[486] On the other hand, a phone survey conducted by the Survey Research Center of the University of California evidenced that the sheer presence of a privacy policy led participants to believe that a business was implementing measures to protect their privacy, regardless of the policy's actual content.[487] While mistakes in judgement do not lead to a legal invalidity of consent, they do call into question the fact, to what extent such authorisations do constitute a true reflection of the individual's wishes. This is why certain forms of Personal Information Management Systems, which will be discussed subsequently, are intended to mitigate these misguided perceptions.

b) Availability

Availability heuristics occur in instances where individuals decide on the probability of a certain event, based on the ease with which such instances come to mind.[488] In that sense, a person who has witnessed or experienced a car accident will most likely provide a higher estimate for the probability of the occurrence of such than someone who has not.[489] This also leads to the so called "hindsight bias", which makes it easier to imagine that an event which has already happened, might occur again.[490] The heuristic of availability can have a quite significant impact on the risk assessment performed by an individual. For example, media coverage which tends to over-

---

[486] *Ur and others*, in: SOUPS '12, 1, 1.

[487] *Hoofnagle/King*, https://ssrn.com/abstract=1262130 (accessed: 13 April 2026).

[488] *Tversky/Kahneman*, 185 Science 1974, 1124, 1127; *Beck*, Behavioral Economics, 28-39.

[489] *Beck*, Behavioral Economics, 39.

[490] *Camerer/Loewenstein*, in: Advances in Behavioral Economics, 3, 10.

emphasise causes of death such as homicides or accidents compared to standard diseases, can lead individuals to largely overestimate the frequency and likelihood of their occurrence.[491]

In the context of privacy conscious choices, data subjects are therefore also likely to heavily rely on their own experiences and those of people close to them, as well as reports in the media. This will, however, for multiple reasons frequently lead to inaccuracies in judgement. First of all, any sort of breaches, incompliance, or fines issued based on the conduct of a controller are far more likely to be reported or noticed by individuals where they concern larger enterprises with a high level of recognition. This might create the incorrect illusion that these are more prone to security incidents or illegal conduct than other less known companies. Secondly, especially in the context of personal data breaches, the fact that these only need to be communicated to the data subject where it is likely to result in a high risk to their right and freedoms (Art. 34(1) GDPR) and do not need to be notified to the supervisory authority where a risk is unlikely to occur (Art. 33(1) GDPR), should be considered. As a result of this, data subjects might be susceptible to a false sense of security, as the actual consequences of a security incident are unlikely to be directly visible or communicated, unless absolutely necessary. On the other hand, this also causes businesses to be even more incentivised against transparent communication of any gaps in their systems or policies, as such might cause data subjects to overestimate both the likelihood and severity of an incident.

c) Anchoring

The anchoring effect refers to the fact that the decisions made by an individual can be influenced by a specific reference point (an anchor).[492] This will potentially become relevant when deciding what

---

[491] *Combs/Slovic*, 56 Journalism Quarterly 1979, 837, 840-842.

[492] *Ni/Arnott/Gao,* 28 Journal of Decision Systems 2019, 67, 67ff; *Rezaei,* 30 Journal of Decision Systems 2020, 72, 72ff; *Calo,* 82 Geo. Wash. L. Rev. 2014, 995, 1012.

type of information to disclose, as studies suggest data subjects might be affected by the actions of their peers, subconsciously viewing these as an "anchor".[493] A 2016 study examining the influence of norm shaping design patterns on the willingness to disclose information found that individuals exposed to more revealing pictures of other users had a tendency to change their personal views on the appropriateness of the sharing of such, increasing the probability of the participants to later publish similar content.[494] Similarly, a 2012 analysis of the impact of relative standards on the propensity to disclose came to the conclusion that individuals were significantly affected by the disclosures made by others, as well as the level of intrusiveness of previously asked questions, both of which serve as a type of "anchor".[495]

Basing a decision-making process on a familiar reference point is not inherently flawed; in some instances it might be quite helpful, even in the context of data privacy. For example, individuals will typically not have an issue with disclosing credit card details during a hotel booking, but might be unwilling to do so when reserving seats for the opera. While technically one could argue that both businesses would have the same right and interest in securing payment in case the person did not show up, the first is a practice typically conducted by businesses and the second one is not. Where a person would therefore be lacking the "anchor" of having disclosed similar data in a similar context, the demand for such might raise red flags and lead the data subject to question the validity of the request. Such instincts should not necessarily be ignored, as they might in fact be helpful. They do, however, also have the potential effect of negatively impacting the reasonableness of our decisions, where the subconscious anchor has no actual bearing on the relevant facts.[496]

---

[493] *Acquisti and others*, 50 ACM Comput. Surv. 2017, 1, 7; *Calo,* 82 Geo. Wash. L. Rev. 2014, 995, 1012.

[494] *Chang and others*, in: 2016 CHI Conference, 587, 587ff.

[495] *Acquisti/John/Loewenstein,* 49 J. Mark. Res. 2012, 160, 160-172.

[496] See for example: *Ariely/Loewenstein/Prelec*, 118 QJE 2003, 73, 73ff, where participants were asked to provide their social security number prior to guessing

d) Privacy Specific Heuristics

Additionally, to these standard heuristics which were first identified in the 1970's and have been largely accepted since then, over the decades the existence of other types of similar mental shortcuts has been established such as, for example, the heuristics of contagion and similarity,[497] common sense,[498] the affect,[499] or scarcity[500]. There have also been attempts to identify specific heuristics relevant for the decision-making process in connection to the willingness to disclose personal data. A review published in 2020, which was based on the existing literature within the field as well as a national survey eliciting the participants' willingness to disclose information about themselves in common online scenarios, identified 12 types of heuristics which were considered distinctly relevant for questions of privacy.[501]

In the social context, the heuristics of (1) authority (a well-known business name can guarantee the security of a website); (2) bandwagon (if most people reveal certain information on a website, I should do this too); (3) reciprocity (if someone provides me with certain details about them, then I should reciprocate in the same manner); (4) sense-of-community (willingness to share information when part of a community); (5) community building (sharing personal information can contribute to community building); and (6) self-presentation (the more information I disclose online, the more I am in control

---

the price for certain products. The study evidenced a significant effect of the individual's number on their subsequent evaluation, although clearly there was no coherent connection between the two.

[497] *Rozin/Nemeroff*, in: Heuristics and Biases, 201, 201ff.

[498] *Ross*, 26 Soc. Epistemol. 2012, 115, 115 ff.

[499] *Slovic/Finucane/Peters/MacGregor*, 177 Eur. J. Oper. Res. 2007, 1333, 1333ff.

[500] *Lynn*, 13 Basic Appl. Soc. Psychol 1992, 3, 3ff.

[501] *Sundar and others*, 2020 CHI Conference, 1, 1ff.

of my online persona) were identified as leading to a stronger willingness to allow the processing of personal data.[502] In the personal context, the heuristics of (7) control (websites providing control over the processing of personal data are safe to use); and (8) instant gratification (an offering in which the service is provided immediately is superior to one where the satisfaction of needs is delayed) were identified as relevant.[503] Finally, with regards to technological context, the heuristics of (9) transparency (where processing operations are transparently described in a privacy policy, the website will be safer); (10) machine (processing of personal data by machines is secure); (11) publicness (the management of personal data in public is not secure); and (12) mobility (mobile devices are inherently unsafe) were found to play an important role.[504]

Whereas these findings are not absolute and the details of certain aspects could potentially be argued, they do evidence an important element, namely that the decision-making process regarding the question of what type of personal data processing individuals allow in general and in the online environment in particular, has been engrained in our everyday life to such an extent that certain specific types of mental shortcuts for these have already been formed. This shows not only the strong effect of the online environment and the connected processing of personal data on each individual's life but also the constant cognitive overload which is experienced in order to make these types of determinations.

3. Biases

Rounding out our inability to form a truly rational decision are cognitive and behavioural biases, which constitute systematic errors in judgement and behaviours, and occur regardless of the complexity

---

[502] ibid 3.
[503] ibid 3f.
[504] ibid 4.

of a specific decision.[505] Whereas heuristics can have the potential to lead to incorrect assumptions or outcomes, they are also generally quite helpful in reducing cognitive overload and do, in fact, frequently result in more or less correct conclusions. Behavioural biases, on the other hand, deviate our thinking from the objective reality and, as per definition, lead us to make counterfactual determinations. Their effect on the decision-making process, with regards to the processing of personal data, therefore needs to be carefully considered.

a) Loss Aversion

Loss aversion has been described as an anomaly in which "the disutility of giving up an object is greater that the utility associated with acquiring it".[506] This, for example, leads to the fact that generally individuals tend to estimate the value of an object as higher if they are in the seller, rather than the buyer position.[507] The effect has, for example, been demonstrated in the context of data privacy in a study, in which data subjects were asked to choose between a $12 gift card, the receipt of which required the provision of personal data, against a $10 gift card, given anonymously.[508] The participants' groups were divided into individuals who had not yet received a specific card and those who already had either one of the gift cards in their possession.[509] The results showed that the proportion of subjects who chose the lower-value anonymous gift card was the highest in the group of participants who already had it in their possession (52.1%).[510] Second and third came the two groups who were given a choice between the two cards without actually receiving one yet,

---

[505] *Haselton/Nettle/Andrews*, in: Handbook of Evolutionary Psychology, 724, 724ff; *Caverni/Fabre/Gonzalez*, 68 Advances in psychology 1990, 7, 7f; *Marshall and others*, 28 TREE 2013, 469, 469ff.

[506] *Kahneman/Knetsch/Thaler*, 5 JEP 1991, 193, 194.

[507] ibid 195-196.

[508] *Acquisti/John/Loewenstein,* 'What Is Privacy Worth?', 42 J. Leg. Stud. 2013, 249, 261.

[509] ibid 261.

[510] ibid 264.

part of which had the $10 card listed first (42.2%) and part second (26.7%).[511] The smallest amount of individuals decided to settle for the anonymous gift card once they already had the higher value in their possession (9.7%).[512] These findings thereby suggest that individuals tend to value their personal data more while it is still in their possession but are generally less likely to accept the incurrence of losses in order to regain such.[513]

b) Status Quo Bias

Loss aversion is also in a sense connected to the so called "status quo bias" which describes a preference of the individual to maintain the current state of affairs. The status quo is hereby taken as a reference point and generally perceived as more positive than other alternatives.[514] The presence of this bias has generally been described as particularly relevant in the fields of politics,[515] ethics,[516] and retirement plans.[517] In the context of data privacy, this will generally result in individuals being less prone to change the already present default setting of online services regarding the processing of their personal data.[518] This can lead to a vast amount of personal data processing being performed without the actual knowledge or awareness of the data subject. It also provides controllers with the potential to include multiple types of processing operations within a layered consent notice, which are subsequently unlikely to be adjusted by the data subject. Surveys conducted in the context of the use of social networks,

---

[511]ibid 264.

[512]ibid 264.

[513]*Acquisti and others*, 50 ACM Comput. Surv. 2017, 1, 7.

[514]*Masatlioglu/Ok*, 121 J. Econ. Theory 2005, 1, 1ff; *Samuelson/Zeckhauser*, 1 J Risk Uncertainty 1988, 7, 7ff; *Hermstrüwer*, 8 JIPITEC 2017, 9, para 8.

[515]*Hong/Lee*, 35 Gov. Inf. Q. 2018, 283, 283ff.

[516]*Bostrom/Ord*, 116 Ethics 2006, 656, 656ff.

[517]*Samuelson/Zeckhauser*, 1 J Risk Uncertainty 1988, 7, 7ff.

[518]*Hermstrüwer*, 8 JIPITEC 2017, 9, para 8; *Acquisti/Grossklags*, in: Digital Privacy Theory, Technologies, and Practices, 363, 373; *Calo,* 82 Geo. Wash. L. Rev. 2014, 995, 1013.

such as Facebook for example, have evidenced a general unawareness of users regarding the existing default settings, as well as their ability to change such.[519]

c) Framing Effects

The framing effect is a cognitive bias based on which individuals will make a different decision regarding the same circumstances and on the form in which it is framed, mainly whether a certain scenario is being presented as a gain or a loss.[520] The significance of its influence on rational decision-making was famously presented through an experiment by Tversky and Kahneman in 1981, in which participants were asked to choose one or two programmes for combating a disease.[521] Although the presented solutions were nearly identical—the only difference was that one was framed in a positive manner (saving 200 out of 600 people) and the other negatively (400 people dying)—respondents clearly favoured the first.[522] The paper also highlighted the relevance of the reference point (i.e. Anchoring) in the context of the individual's decision-making process.[523] The framing effect has since then been widely recognised as an important cognitive bias and its significant effect on the decisions of individuals further highlighted.[524]

aa) Influence on the Data Subject

The same effect has also been evidenced to influence decisions made by data subjects regarding the processing of their personal

---

[519] *Acquisti/Gross*, in: PET 2006, 36, 36ff; *Gross/Acquisti*, in: WPES '05, 71, 71ff.

[520] *Gong and others*, 18 Psychol Health Med 2013, 645, 645ff.

[521] *Tversky/Kahneman*, 211 Science 1981, 453, 453ff.

[522] ibid 453.

[523] ibid 456.

[524] See for example: *Druckman*, [22] J. Econ. Psychol. 2001, 91, 91ff; *Levin/Schneider/Gaeth*, 76 Organ. Behav. Hum. Decis. Process. 1998, 149, 149ff; *Kühberger*, 75 Organ. Behav. Hum. Decis. Process. 1998, 23, 23ff; *Peng/Guo/Hu*, 9 Vaccines 2021, 995, 995 ff.

data. Experiments conducted in the field have shown that notices framed as increasing in protection lead to more frequent disclosures in personal data, whereas those framed as decreasing reached the opposite outcome.[525] Similarly, a decline of disclosures connected to privacy notices describing processing activities involving higher risk could be muted or significantly reduced through the introduction of slight misdirections which did not, however, alter the objective risk of the disclosure.[526] Quite interestingly, especially in the context of Personal Information Management Systems, individuals seem to be more willing to share information when they are given more control over its release.[527] Such an increase of (perceived) information control has also been indicated to reduce general concerns for privacy.[528] While tendencies in increasing user control are to be supported, the general ramifications of the framing effect in the field of data privacy have been largely disruptive. The immense potential of affecting users' choices through the form and wording in which facts are presented leads to serious questions as to the extent to which such consent can still be considered as "freely given" and "informed" under such circumstances.

bb) Nudging and Dark Patterns

The potential of affecting users' decisions through the implementation of positive framing techniques has not gone unnoticed by business and has led to the utilisation of so called "nudging" practices and "dark patterns" on a large scale, especially in the context of online consent banners.[529] The term "nudging" was largely popularised by the 2008 publication "Nudge: improving decisions about

---

[525] *Adjerid and others*, SOUPS '13, 1, 10.

[526] *Adjerid and others*, SOUPS '13, 1, 10.

[527] *Brandimarte/Acquisti/Loewenstein*, SPPS 2013, 340, 345f.

[528] *Taylor/Davis/Jillapalli*, 9 JECR 2009, 203, 218f.

[529] *Loy/Baumgartner*, 8 ZD 2021, 404, 404; *Denga*, 3 ZfDR 2022, 229, 230; *Weinmann/Schneider/vom Brocke,* 58 Bus Inf Syst Eng 2016, 433, 434f.

health, wealth and happiness" and generally does not have a negative connotation.[530] It refers to the practice of gently steering individuals towards making decisions which have a positive effect, either on their own well-being or that of society as a whole.[531] Dark patterns, also known as "deceptive design patterns" on the other hand are inherently negative as they describe user interfaces which have been purposefully crafted in order to trick users into doing something they did not intend or would not have done under normal circumstances.[532] In the context of privacy notices and consent banners these are, for example, introduced in the form of hiding interface elements which allow the selection of privacy friendly choices, asking questions regarding the users' preferences in a purposefully confusing manner, or creating an illusion of choice by connecting the requirement for consent to "irresistible" benefits.[533]

Whereas clear, purposeful traps or deceptions forcing users to provide consent contrary to their intention will naturally be considered incompliant with the requirements of the GDPR, a large amount of practices, especially in the context of "gently steering" users into the disclosure of their personal data, can be found on the market. These are not be considered illegal but clearly do intend to affect the user's choice.[534] Especially popular in that regard are practices such as using specific colours to steer users' attention towards a specific selection button, not including the option to reject the use of cookies on

---

[530] *Thaler/Sunstein*, Nudge.

[531] *Barton/Grüne-Yanoff*, 6 Rev. Philos. Psychol. 2015, 341, 342ff; *Hagman and others*, 6 Rev. Philos. Psychol. 2015, 439, 440ff; *Sunstein*, 6 Rev. Philos. Psychol. 2015, 511, 511.

[532] *Luguri/Strahilevitz*, 43 Journal of Legal Analysis 2021, 43, 43ff; *Narayanan and other*, 18 Queue 2020, 67, 67ff; *Day/Stemler*, 72 Alabama Law Review 2020, 1, 1ff.

[533] *Nouwens and others*, CHI '20, 1, 2; *Waldman*, 31 Current Opinion in Psychology 2020, 105, 107.

[534] *Christine Utz and others*, 'CCS '19, 973, 976 found that 57.4 % of reviewed consent notices applied an interface design, which steered website visitors towards accepting privacy unfriendly options.

the first layer, having to manually deselect a large number of potential recipients, or interfering with the withdrawal of consent.[535] Some of these elements, such as the incorporation of pre-ticked boxes or "cookie walls", have by now been explicitly confirmed as illegal;[536] the validity of elements such as the use of certain colours or fonts are still being debated.[537] Here the question often occurs how far such solutions are in fact allowed to go before being deemed as unlawful, often effectively blurring the line between a "nudge" and a "dark pattern". Quite interesting in that context are new developments in research which attempt to reach the quite opposite effect, namely nudging users towards privacy friendly options. Those will, however, be discussed under Part 1 Chapter 2: C. IV. Proposals for Improvement subsequently, as they constitute a remedy rather than a hindrance, and also go beyond the use of framing effects by applying solutions such as defaults and incentives

d) Immediate Gratification and Hyperbolic Discounting

Per definition, hyperbolic discount functions are described as "a relatively high discount rate over short horizons and a relatively low discount rate over long horizons".[538] Effectively, this means that individuals will typically present a stronger preference for more immediate payoffs, rather than such which occur later.[539] This discount func-

---

[535] *Bermejo Fernandez and others*, 5 Proc. ACM Hum.-Comput. Interact. 2021, 1, 1ff; *Christine Utz and others*, 'CCS '19, 973, 976-982; *Bösch/Erb/Kargl/Kopp/Pfattheicher*, PoPETs 2016, 237, 237ff.

[536] *EDPB*, Guidelines 05/2020, para 39; *Art. 29 WP*, Working Document 02/2013, 5; *DSK*, *Orientierungshilfe Telemedien*, para 42; Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 62f.

[537] *Hanloser*, 7 ZD 2019, 287, 287ff; *Sesing*, 7 MMR 2021, 544, 546; *Ettig/Herbrich*, 11 K&R 2020, 719, 720 *Baumgartner / Hansch,* ZD 2020, 435, 437; *Haberer*, MMR 2020, 810, 813-814; *Loy/Baumgartner*, 8 ZD 2021, 404, 404ff.

[538] *Laibson*, 112 QJE 1997, 443, 445; *Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 220.

[539] *Hermstrüwer*, 8 JIPITEC 2017, 9, para 47; *O'Donoghue/Rabin*, 116 QJE 2001, 121, 123.

tion is, however, not linear as individuals, while overvaluing proximate satisfactions, are able to recommit to more logical and positive resolutions in the future.[540] This means that where, for example, a person would be given a choice between eating one apple now or two tomorrow, most would be prone to choosing immediate satisfaction, rather than the larger payoff at a later time.[541] If, on the other hand, having the choice between receiving one apple in one year or two apples in one year and one day, logically, most would decide to wait the additional day.[542] Although the two options are technically identical, when it comes to the promised payoff and the additional time necessary to wait for such, the preferences of individuals in the two scenarios are diametrically different. This phenomenon is also commonly described as a "dynamic inconsistency", as individuals make conflicting choices over time.[543]

These biases are also profoundly relevant in the context of consumer decision-making in relation to the processing of their personal data, especially where the person is faced with a visible gain resulting from the disclosure of the relevant information, such as access to a social interaction, a game or a discount. For example, in an experiment conducted in a study analysing the monetisation of privacy, participants were given the option to choose between two different websites to buy a movie ticket, with one requesting more personal information (phone number) or using it for additional purposes (advertising), while at the same time offering the ticket for a lower price (50 cents less). [544] This was on average preferred to the cheaper option, for the price of data disclosure.[545] The effect of hyperbolic discounting is even more exacerbated in that context, since the potential loss incurred from the disclosure is so intangible and the risks

---

[540] *Strotz*, 23 REStud 1995, 165, 177.

[541] *Thaler*, 8 Econ. Lett. 1981, 201, 202.

[542] ibid 202.

[543] *Moloi/Marwala*, Artificial Intelligence, 43-52; *Thaler*, 8 Econ. Lett. 1981, 201, 201-207.

[544] *Jentzsch/Preibusch/Harasser*, Study on monetising privacy, 29-33.

[545] ibid 33.

do not only lie in the future, but are also uncertain. This is why the immediate gratification syndrome is also frequently considered as one of the explanations for the above-mentioned privacy paradox.[546] After all, it is in a sense logical to select an immediate gain over a theoretical unclear risk.

Businesses have also learned to effectively take advantage of that fact, conveniently placing consent banners in a way that potentially interferes with the consumption of the desired service or content, leading users to quickly accept all types of cookies and tracking mechanisms in order to quickly meet their needs.[547] Whereas typical "cookie walls" blocking access to a website where not strictly necessary cookies are not being accepted, are prohibited,[548] there are still multiple ways in which the specific positions of a banner have been proven to influence user behaviour.[549] This can have disastrous effects, where data subjects decide to disclose personal information for seemingly small pleasures, which can lead not only to regret but also entail potentially serious ramifications such as price discrimination, the loss of job offerings, or even identity theft.[550] In that sense, the presence of information asymmetries is also furthering the effect of these already inherently present biases.[551]

---

[546]*Acquisti*, EC '04, 21, 21ff *Barth/de Jong*, 34 TELEMAT INFORM 2017, 1038, 1047; *Acquisti and others*, 50 ACM Comput. Surv. 2017, 1, 9; *Gerber/Gerber/Volkamer*, 77 Comput. Secur. 2018, 226, 230.

[547]*Christine Utz and others*, 'CCS '19, 973, 975; *Schaub and others*, SOUPS 2015, 10.

[548]*EDPB*, Guidelines 05/2020, para 39; *Art. 29 WP*, Working Document 02/2013, 5; *DSK*, *Orientierungshilfe Telemedien,* para 54.

[549]For example, there are findings indicating that website visitors are most likely to interact with a consent banner where such is placed on the bottom left, whereas a positioning on the top of a website generally yields low interaction rated. See: *Christine Utz and others*, 'CCS '19, 973, 974.

[550]*Wang and others*, in: SOUPS '11, 1, 1-6; *Acquisti/Fong*, 66 Manag. Sci. 2020, 1005, 1005ff; *Acquisti and others*, 50 ACM Comput. Surv. 2017, 1, 9.

[551]*Hermstrüwer*, 8 JIPITEC 2017, 9, para 32; *Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 222.

e) Optimis Bias and Overconfidence

Also contributing to the effects of hyperbolic discounting and dynamic inconsistency are the biases of optimism and overconfidence. These two lead to a tendency to both underestimate the likelihood of experiencing a negative effect, as well as overestimate the accuracy of one's own judgements in that regard.[552] This can also serve as an explanation for the privacy paradox, as additionally to preferring the immediate receipt of a gain over the consideration of the future risk, data subjects might be prone to underestimate the actual potential of such risks occurring in the future, as well as overestimate their own capabilities in assessing such.[553] The relevance of this bias in the context of data privacy has been confirmed by a study examining the ways in which risk judgements about the protection of personal data are being constructed by internet users.[554] Here the participants were asked questions regarding their perceived personal vulnerability for privacy related risks ("How likely are you to become the victim of an invasion of online privacy?" and ''How likely is it that your personal information will be stolen over the Internet?"), as well as those incurred by society in general.[555] The final results showed that respondents were not only confident in their own ability to control their privacy online but also had a strong tendency to believe that they were less likely to experience any risks in that context, than others.[556] This can lead to potentially careless behaviour, even in more privacy conscious individuals.

---

[552]*Irwin*, 21 Personality 1953, 329, 329ff; *O'Sullivan*, 8 Dial Phil Ment Neuro Sci 2015, 11, 11ff; *Chapin/Coleman*, 11 N. Am. J. Psychol. 2009, 121, 121ff; *Weinstein/Klein*, 15 J. Soc. Clin. Psychol. 1996, 1, 1ff; *Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 219.

[553]*Barth/de Jong*, 34 TELEMAT INFORM 2017, 1038; *Acquisti and others*, 50 ACM Comput. Surv. 2017, 1, 9; *Gerber/Gerber/Volkamer*, 77 Comput. Secur. 2018, 226, 229.

[554]*Cho/Lee/Chung*, 26 CHB 2010, 987, 987ff.

[555]ibid 990.

[556]ibid 990.

4. Consent Fatigue

Another element posting a significant hindrance with regard to the collection of truly free, specific, informed, and unambiguous consent is the phenomenon described as “consent fatigue”.

a) Background

Online services have become an integral part of most lives; they are used not only solely for entertainment but also for crucial aspects such as online banking, tax statements, booking doctor’s appointments, ordering all types of goods, as well as work, research and social interactions. However, as soon as the processing operations of the service provider are intended to go beyond what is strictly necessary for the provision of a particular service, the need to base the use of such personal data on another legal basis than Art. 6(1)(b) appears. Whereas legitimate interest under Art. 6(1)(f) can theoretically constitute a valid legal basis under the GDPR, the application of such is largely problematic due to the requirements introduced by “Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector”, also known as the E-Privacy Directive.

Article 5(3) therein provides that “Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent”.[557] This requirement for the collection of consent

---

[557]The requirement for consent, was not originally included in the wording of Art. 5(3), but introduced though an amendment in 2009. See: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

has historically been subject to a heated debate between privacy professionals regarding the relationship between the two legal acts, most importantly whether GDPR compliant consent was necessary for the deployment of cookies and other tracking techniques.[558] This conflict, however, has been largely resolved through the CJEU's ruling on Planet 49, where the court concluded that GDPR-compliant consent is in fact necessary for storing information or gaining access to such saved on the terminal equipment of an end-user.[559]

b) Consequences

In consequence, controllers are obliged to collect an individual's consent where they wish to apply any type of cookies or other tracking techniques which are not strictly necessary for the provision of a service.[560] Also, as outlined above, valid consent needs to be sufficiently granular, meaning all purposes need to be separately listed

---

[558] *Haberer*, MMR 2020, 810, 811f; *Rauer/Ettig*, 6 ZD 2015, 255, 257f; *Schmidt/Babilon*, 2 K&R 2016, 86, 86-90; Hoeren/Sieber/Holznagel / *Schmitz*, 'Teil 16.2 Datenschutz im Internet' in Thomas Hoeren, Ulrich Sieber and Bernd Holznagel, HdB MultimediaR, Teil 16.2, para 274-277.

[559] The Case concerned the validity of a pre-selected check box allowing Planet 49 to set cookies enabling the tracking and evaluation of users' online behaviour. In that context the Court ruled that: "*In the light of the foregoing considerations, the answer to Question 1(a) and (c) is that Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, must be interpreted as meaning that the consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent*". See: Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 65.

[560] *Rauer/Ettig*, 1 ZD 2021, 18, 18ff; *Spindler*, 35 NJW 2020, 2513, 2513ff; *Böhm/Halim*, 10 MMR 2020, 651, 654.

and individuals should be given the option to only select the operations to which they wish to agree, omitting others.[561] Furthermore, pre-ticked boxes and inactivity are clearly excluded as they do not constitute unambiguous behaviour (see Part 1 Chapter 2: C. I. 4. Unambiguous). In turn, as businesses do have a strong interest in tracking their consumers' online conduct, data subjects are confronted with a consent banner for the collection of personal data at basically any website they enter. Paired with the extensive use of online services in general, this effectively leads individuals to be confronted with repetitive consent requests at each step, both for critical and minor processing of personal data.[562]

This naturally leads not only to basic aggravation but also to previously mentioned cognitive overload, as it is virtually impossible for a person to seriously consider the content and ramifications of each single processing for each website they visit.[563] As a result, consumers have reported feeling a general loss of control, leading them to emotional exhaustion and cynicism with regard to the management of their online privacy.[564] After all, these notices in a sense stand in the way of the primarily pursued goal, namely the usage of the service.[565] Due to that, consent notices have become largely meaningless to users,[566] with many simply choosing to "click away"

---

[561] *EDPB*, Guidelines 05/2020, para 42; ; *Brüggemann/Hötzel*, in: Sozialdatenschutz in der Praxis, para 111f; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 6; Rücker/Kugler, *Dienst*, C. Lawful processing, para 448.

[562] *Mali*, 7 Int. J. Law 2021, 142, 146.

[563] *Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 220; *Vidhani/Banahatt/Lodha*, 9 CSIT 2021, 185, 190; *von Grafenstein and others*, Regulation through, 5; *Porat/Strahilevitz*, 112 MLR 2014, 1417, 1472.

[564] *Choi/Park/Jung*, 81 Comput. Hum. Behav. 2018, 42, 42ff; *Tian/Chen/Zhang*, 12 Applied Sciences 2022, 9702, 4.

[565] *Nouwens and others*, CHI '20, 1, 10; *Christine Utz and others*, 'CCS '19, 973, 973.

[566] *Schaub and others*, SOUPS 2015, 3.

consent banners[567] as fast as possible, either opting for general rejections or acceptance of all purposes, without ever reading any of the provided details, thereby effectively creating the illusion of consent rather than allowing legitimate data processing on the basis of Art. 6(1)(a) GDPR.

5. Interim Conclusions: Behavioural Obstacles

As outlined above, there are a number of aspects largely inherent to human behaviour that are effectively hindering many (not all) data subjects from making rational decisions about the processing of their personal data. This can result both from mental shortcuts, performed in order to mitigate cognitive overload (heuristics), and cognitive and behavioural biases, which deviate our thinking from the objective reality and cause us to make systematic errors in judgement. Further aggravating these issues is the frequency by which individuals are being asked to deal with controllers' requests for consent, effectively leading users to be fatigued with such and largely resulting in complete disregard for most displayed banners. These phenomena have been used to explain the generally observed "privacy paradox", demonstrated in the fact that the behaviours of data subjects, especially in the online environment, are largely inconsistent with their declared privacy preferences. These outlined hindrances, as well as multiple others, have led to an extensive criticism of this legal concept in general.[568]

---

[567] *Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 220; https://jusletter.weblaw.ch/juslissues/2018/924/profiling-in-the-gdp_3b8e8a124f.html__ONCE&login=false (accessed: 04 March 2026).

[568] *Richards/Hartzog*, 96 WULR 2019, 1461, 1461ff; *Efroni and others*, 5 EDPL 2019, 352, 355-357; *Hacker*, Datenprivatrecht, 255-258; *Jarovsky*, 4 EDPL 2018, 447, 448-451; *Koops*, 4 IDPL 2014, 250, 251ff; *Blume*, 2 IDPL 2012, 26, 29-32; *Haase*, 3 InTeR 2019, 113, 113ff.

IV. Proposals for Improvement

As evidenced above, consent as a legal basis is intrinsically linked to the realisation of the right to self-determination and at the same time, is integral and unavoidable for the average consumer entering the online realm. Furthermore, it is inherently flawed based on many practical hurdles as well as behavioural aspects. Based on this, much research and effort has been put into discussions on how to mitigate these issues, enhance the user experience, and enable the collection of truly free, specific, informed, and unambiguous consent.[569] One proposed remedy relates to the hope that Personal Information Management Systems, in the form of user operated consent platforms, will be able to solve these issues.[570] Therefore, solutions which are currently being contemplated and worked on in that context shall be analysed below. As always, the selected examples are, however, only used in order to illustrate general tendencies, considerations and developments, and cannot be considered as exhaustive or final.

1. OPERANDO and PlusPrivacy

OPERANDO, which stands for Online Privacy Enforcement, Rights Assurance and Optimization, was a research project largely funded under the Horizon 2020 Framework Programme for Research and Innovation between May 2015 and April 2018.[571] The project intended to "specify, implement, field-test, validate and exploit an innovative privacy enforcement platform", enabling Privacy

---

[569] *Efroni and others*, 5 EDPL 2019, 352, 357-364; *Jarovsky*, 4 EDPL 2018, 447, 447ff; *Pandit*, https://arxiv.org/abs/2208.05786 (accessed: 25 March 2026); *Hacker*, Datenprivatrecht, 578-619; *Pardo/Le Métayer*, Inria Rhone-Alpes 2019, 1-22.

[570] *Attoresi/Moraes*, TechDispatch #3/2020, 2; *Riechert/Richter*, Was die DSGVO braucht, 8-10; *EDPS*, Opinion 9/2016, para 25-28.

[571] OPERANDO, https://cordis.europa.eu/project/id/653704 (accessed: 14 October 2025).

as a Service.[572] The main identified objectives set out by the consortium were (1) enabling user-friendly privacy enforcement; (2) the implementation of Privacy-by-Design; (3) the creation of viable business and trust models; (4) the demonstration and validation of the solution; and (5) the assurance of a sustainable framework.[573] While also delivering a privacy enforcement platform available as a service from public bodies, proposing a legally motivated privacy framework, and supporting a business model under which Privacy Service Providers (PSPs) use the software to offer Privacy as a Service, these elements are only to a limited extent relevant in the context of this thesis.[574]

What is, however, quite significant is the creation of the "Plus Privacy" application which provides a data subject with a unified dashboard, allowing them control over the privacy settings in social media accounts.[575] Currently, individuals are given the option to configure all data privacy settings on Google, Facebook, Twitter and LinkedIn at once, while also retaining the option to adjust those individually.[576] Although being able to adjust privacy preferences over multiple platforms is likely easier than doing so separately on the web page of each of the providers, it should be noted that the practical effect of this functionality in limiting the cognitive overload for data subjects is likely to be quite minimal. After all, the person in question will still have to go to the trouble of finding, downloading and installing the application, only to be able to set-up privacy settings for an entirety of four data controllers. While Plus Privacy also contains other functionalities such as ad blocking, as well as preventing malware and unwanted apps or browser extensions from processing the individual's personal data through tracking or other means,[577] these are not

---

[572]ibid.

[573]OPERANDO: Periodic Reporting for period 2, https://cordis.europa.eu/project/id/653704/reporting (accessed :14 October 2025).

[574]ibid.

[575]PlusPrivacy, https://plusprivacy.com/ (accessed: 14 October 2025).

[576]PlusPrivacy FAQ, https://plusprivacy.com/faq/ (accessed: 14 October 2025).

[577]PlusPrivacy, https://plusprivacy.com/ (accessed: 14 October 2025).

necessarily different from similar solutions already available on the market. In that sense, the App should be considered as a good starting point rather than a fully developed Personal Information Management System, reducing the burdens put on individuals in the online environment.

2. World Data Exchange

The services offered by "World Data Exchange" will also be mentioned in the context of the right to data portability in the following (see Part 1 Chapter 2: D. II. 5. f) bb) (3) World Data Exchange), since they allow users to retrieve data from multiple controllers and transfers such into a standardised JSON file format.[578] Once their data has been retrieved, users are additionally encouraged to further share their data through one of the provider's apps.[579] The application also contains a specific consent feature intended to allow the collection of explicit and informed user consent by laying down all relevant information in a clear manner *via a* standardised consent screen.[580] In that sense, both the behavioural obstacles discussed in this section (see Part 1 Chapter 2: C. III. Behavioural Obstacles) and such previously outlined in the context of transparency (see Part 1 Chapter 2: B. II. Obstacles) are being tackled at once.[581] The standardised interface for all businesses requesting access to the user's personal data, as well as the utilisation of icons, support the general intelligibility of the provided information. On the other hand, a uniform look allows the avoidance of framing effects and can potentially support the reduction of certain biases. Furthermore, individuals decid-

---

[578]World Data Exchange, https://worlddataexchange.com/demo (accessed: 22 October 2025).

[579]World Data Exchange, https://worlddataexchange.com/feature-consent (accessed: 22 October 2025).

[580]World Data Exchange, https://worlddataexchange.com/feature-consent (accessed: 22 October 2025).

[581]Demo versions of the displayed consent screens can be viewed under https://try.digi.me/sources (accessed: 14 October 2025).

ing to download the application will have the option to set their preferences for multiple service providers in one go. While the amount of decisions to be made is not reduced through that fact alone, it does allow the data subject to set aside some time for the determination of these preferences in a calm manner, rather than constantly confronting them with such a request, as it is currently the case in the online environment. In that sense, the effects of consent fatigue might also to a certain extent be reduced. The platform, however, is also only able to facilitate the management of the individual's personal data for controllers who have previously signed up with the platform.[582] While the amount of "data sources" which can be managed through the service is significantly higher than was the case with the Plus Privacy App,[583] this ultimately still creates as strong dependency on the cooperation of data controllers, in a sense limiting the "user centric" character intended for Personal Information Management Systems.

3. MyDex

The platform services currently offered by MyDex include: (1) a Personal Data Store, used for the collection, retrieval and storage of personal information; (2) a Personal Data Exchange Service, adding the possibility of distributing such between organisations and other parties; (3) Identity as a Service, allowing secure authentication; (4) an included Platform, enabling two-way engagement between individuals and controllers; and (5) a Web App Generator, providing a tool for transforming manual services into digital applications.[584] The Personal Data Store of each individual is kept independently of any

---

[582]Controllers can register under the following under https://worlddataexchange.com/ (accessed: 14 October 2025).

[583]As of October 2024, the platform facilitated data management for over 5,000 sources of hospital and GP records, over 1,000 for banking transactions and over 10 for fitness, wellbeing, and social interests: https://worlddataexchange.com/comprehensive-data-sources (accessed: 14 October 2024).

[584]https://mydex.org/platform-services/ (accessed: 03 March 2026).

data collection from contro hich enables the collection, delivery and distribution of information between data subjects and controllers through secured channels.[585] Additionally, other llers, which is facilitated through unique and separate encryption keys.[586] The platform itself operates on a "zero knowledge philosophy", with no access to the information.[587]

Serving as a form of consent management platform is the Personal Data Exchange service, w data subject rights connected to consent management such as erasure (this is, for example, to be achieved through individualised encryption keys, see Part 1 Chapter 2: D. II. 3. c) bb) (2) Revocation)[588] or portability are also supported.[589] Direct engagement between data subjects (here called citizens) and organisations is facilitated through the Included Platform for which individuals sign up before starting their engagement with local service providers.[590] These businesses, also referred to as "subscribers", have the option to present incentives and offers as well as seek feedback or direct engagement from their already present client base in order to gain insights and improve the targeting of their services.[591] All personal data is provided by the data subjects as part of a sharing agreement and is under the constant control of the individual.[592] Also, where data was originally provided via the platform,

---

[585] https://mydex.org/platform-services/ (accessed: 03 March 2026).

[586] https://mydex.org/resources/papers/AchievingTransformationAtScale/AchievingTransformationatScaleMydexCIC-2021-04-14.pdf (accessed: 03 March 2026).

[587] ibid.

[588] *Papadopoulou and others*, in: Agent and Multi-Agent Systems, 239, 241f.

[589] https://mydex.org/resources/papers/Data_portability_white_paper/mydexcicdataportabilitywhitepaper2018-06.pdfhttps://mydex.org/resources/papers/Data_portability_white_paper/mydexcicdataportabilitywhitepaper2018-06.pdf (accessed: 03 March 2026).

[590] https://mydex.org/platform-services/#mrd (accessed: 03 March 2026).

[591] ibid.

[592] ibid.

its re-collection, transmission and further distribution will be possible.[593]

4. Meeco

Also offering a form of consent management is the provider Meeco.[594] The core capabilities of this "Secure Value Exchange" platform are (1) Secure Data Storage; (2) Verifiable Credentials; and (3) Digital Assets.[595] The Vault for secure data storage guarantees end-to-end encryption in transit and rest, as well as GDPR compliant hosting within the European Union for customers located there.[596] It is possible to embed the vault into existing applications through authentication with an OpenID Connect provider.[597] Organisations are also given the option to share personal data with their customers, for example, for compliance with data subject requests for access or portability via the platform in a secure manner.[598]

The consent and permissions management functionality, most relevant in this context, allows individuals to share data with other individuals, as well as organisations through a secure and private channel.[599] Any adjustments or updates to information made in the system will also be automatically applied on the recipient's side.[600] Consent for access to the users' personal data can also be provided in a quite granular and specific manner, allowing specific elements to be determined such as the duration of the access or the extent to which forwarding and on-sharing are allowed.[601] These set-ups made by the data subject are then enforced by the platform.[602]

---

[593]ibid.
[594]https://www.meeco.me/ (accessed: 03 March 2026).
[595]ibid.
[596]https://www.meeco.me/platform (accessed: 03 March 2026).
[597]ibid.
[598]https://docs.meeco.me/guides/organizations (accessed: 03 March 2026).
[599]ibid.
[600]ibid.
[601]https://www.meeco.me/platform (accessed: 03 March 2026).
[602]ibid.

While these functionalities are likely capable of supporting easier control of the user's personal data, the set up of such an account is quite complicated and can therefore hardly be described as user friendly. As a first step, developers need to sign up at the Meeco Developer Portal.[603] Once they have followed the procedure therein, confirmed the account via e-mail and logged in, they receive a subscription name, are presented with the Terms of Use, and can subscribe to the service.[604] This will then allow the generation of the keys, necessary for the generation of requests via the developer portal.[605] Only then will developers be able to generate users and items for the digital vault by following a number of commands.[606] Considering the number of steps necessary for the set up of a vault, as well as the technical knowledge required for such, it is unlikely that individual users, especially those without any IT-knowledge, will initiate the creation of this themselves. Thus, data subjects are still largely dependent on the controller to implement this solution, limiting the "user enabling" effect of this particular PIMS.

5. Advanced Data Protection Control

Advanced Data Protection Control (ADPC) was initiated as part of the RESPECTeD project which was funded as part of a collaboration between the Sustainable Computing Lab[607] and noyb.[608] Its original aim was to develop novel mechanisms for the communication of individuals' privacy and tracking preferences.[609] The project has since grown with the group of collaborators including individuals from the

---

[603] https://docs.meeco.me/latest/getting-started/setting-up (accessed: 03 March 2026).

[604] ibid.

[605] https://docs.meeco.me/latest/getting-started/setting-up (accessed: 03 March 2026).

[606] https://docs.meeco.me/latest/getting-started/quickstart (accessed: 03 March 2026).

[607] https://www.sustainablecomputing.eu/ (accessed: 03 March 2026).

[608] https://noyb.eu/en (accessed: 03 March 2026).

[609] https://www.respected.eu/ (accessed: 03 March 2026).

fields of computer and cognitive science, social studies, and law and digital rights activism, who are "working together to empower humans in the digital world".[610]

The ADPC constitutes an automated mechanism through which users can provide, refuse or withdraw consent for the processing of their personal data in the online environment.[611] It also allows users to object to processing based on legitimate interest in the same manner.[612] This is intended primarily to remedy the current way of collecting personal data through the use of "cookie banners",[613] since these are commonly known to lead to consent fatigue and exploit biases such as framing effects, immediate gratification, and hyperbolic discounting, as described above.[614] Instead of being confronted with a consent request at each interaction with a website, data subjects are able to configure their privacy preferences in advance, which are then communicated towards the provider without interrupting the online experience.[615] Individuals can decide when they would in fact be presented with consent requests or when such should either be automatically denied or accepted.[616] All of these settings can be accessed and amended at any time via a specific user interface.[617]

The tool's functionalities are facilitated through the exchange of HTTP headers between the data subject and the relevant web server,[618] or alternatively with an equivalent JavaScript interface.[619]

---

[610] https://www.dataprotectioncontrol.org/ (accessed: 03 March 2026).
[611] https://www.dataprotectioncontrol.org/about/ (accessed: 03 March 2026).
[612] ibid.
[613] https://www.dataprotectioncontrol.org/ (accessed: 03 March 2026).
[614] See Part 1 Chapter 2: C. III. 3. Biases and 4. Consent Fatigue.
[615] https://www.dataprotectioncontrol.org/ (accessed: 03 March 2026).
[616] https://www.dataprotectioncontrol.org/spec/#concept (accessed: 03 March 2026).
[617] https://www.dataprotectioncontrol.org/ (accessed: 03 March 2026).
[618] https://www.dataprotectioncontrol.org/spec/#concept (accessed: 03 March 2026).
[619] https://www.dataprotectioncontrol.org/spec/#concept (accessed: 03 March 2026).

As will, however, be discussed in the context of the right to objection, the implementation of similar techniques such as Do-Not-Track mechanisms, has already been attempted in the past but mostly failed due to both technical and legal barriers.[620] In that sense, it remains to be seen whether the proposed solution will be able to prevail in the long run. The creators have argued that the current approach is superior to previous attempts since it integrates the requirements of the GDPR and the upcoming ePrivacy Regulation into the functionalities.[621] To this end, they list multiple characteristics of the ADPC, which distinguish it from other solutions.

First of all, the Advanced Data Protection Control is domain specific, which means that data subjects are able to adjust their preferences for selected websites or data controllers.[622] It also allows both the acceptance and rejection of a consent request instead of simply blocki*ng any type of tracking mechanisms, and while the signals can be set in a generalised "accept all" or "reject all" manner, they allow for more specific determinations (for example, rejecting certain purposes while allowing* others) as well.[623] Furthermore, the Control does not require domains to use a formulation for the consent request standardised by industry groups but rather allows them to define them freely, making it more open and interoperable with other systems.[624]

Considering these crucial advancements, it will be interesting to see if the proposed solution will be able to gain more practical relevance than its predecessors. As of the time of writing, the Advanced Data Protection Control is still at a proof-of-concept status and is mainly intended to constitute a starting point for a wider debate on the facilitation of data subject rights through the adaption browser

---

[620] See Part 1 Chapter 2: D. II. 6. c) aa) (2) (a) Do Not Track.
[621] https://www.dataprotectioncontrol.org/about/ (accessed: 03 March 2026).
[622] ibid.
[623] ibid.
[624] ibid.

signals.[625] While the platform is therefore not actually functional, a prototype is already available for download.[626]

6. PRIVACY-AVARE

Another research project also working on the creation of software which would allow the transfer of a user's pre-determined privacy preferences onto all of their terminal equipment, is AVARE.[627] The essential elements of the application are the creation of the user's personal preference profile, the distribution of the profile to the consumer's devices, and the enablement of the control of data access.[628] The access authorisations are being facilitated through monitoring all requests at runtime and blocking data flows in accordance with the rules set out by the data subject, extracting information from existing resources (such as address books), and incorporating permission settings of existing applications.[629]

The most recently presented component enforcing user preferences is referred to as the "AVARE-Box". This comprises a sandbox which constitutes an isolated environment in which an application can be amended without causing any effect on the production environment and a reference monitor, which allows communication between the application in the sandbox and the operating system.[630] The argumentation of the communication in accordance with the predefined preferences is facilitated through the use of hooking operations.[631] Based on this, the reference monitor is able to first forward application requests to the operating system, and then adjust and

---

[625] ibid.

[626] https://www.dataprotectioncontrol.org/prototype/ (accessed: 03 March 2026).

[627] *Alpers and others*, in: FrOSCon 2018, 2, 2ff.

[628] *Alpers and others*, in: CLOSER 2018, 589, 591f; *Alpers and others*, in: FrOSCon 2018, 2, 4 f.

[629] *Alpers and others*, in: CLOSER 2018, 589, 592.

[630] *Alpers and others*, in: FrOSCon 2018, 2, 4.

[631] ibid 4f.

filter the provided answers in accordance with the user's settings before delivering an answer to the app.[632] Currently three plug-ins have been enabled in the AVARE-Box: a Contacts-Filter-Plug-in, a Location-Filter-Plug-in, and a Calendar-Filter-Plug-in.[633] The complete technical implementation of the tool is, however, still impeded by significant hindrances as currently separate strategies need to be applied for each operating system platform and at times, multiple versions and strategies have to be selected within one system.[634]

7. Effectivness

In the context of analysing these proposed solutions, the question arises to what extent these are actually capable of mitigating the problems described under Part 1 Chapter 2: C. III. Behavioural Obstacles. On the one hand, adjusting and standardising the form in which information about the processing activities is being presented may support the individual in forming an understanding of the planned activity and thereby mitigate cognitive biases to a certain extent. Especially, the impact of framing effects (see Part 1 Chapter 2: C. III. 3. c) Framing Effects) could be significantly reduced by presenting the same information in a more objective manner. Also, since the reliance of heuristics is mainly the result of experiencing cognitive overload,[635] a more simplified presentation may support the individual in the determination process. In that sense, the impact of such consent management tools is very similar to the reductive potential discussed in the context of transparency enhancing technologies previously (see Part 1 Chapter 2: B. III. 1. e) Reductive Potential).

---

[632] ibid 5.

[633] ibid 7.

[634] ibid 11.

[635] *Knauff*, in: Rationale Entscheidungen, 15, 15; *Beck*, Behavioral Economics, 25f.

Still, these positive effects will not extent to all users.[636] After all, the reasons as to why users make certain decisions are as varied as the individuals themselves.[637] Especially those struggling with consent fatigue are more interested in reducing their exposure to consent notices overall, rather than improving them.[638] Tools such as Plus Privacy (see Part 1 Chapter 2: C. IV. 1. OPERANDO and Plus Privacy), allowing the set up of privacy preferences across multiple platforms, might be more effective in that regard. They would, however, need to include more data controllers within their service than is currently the case. Also, studies conducted on tools intended to support individuals in limiting online behavioural advertisements have identified serious usability flaws.[639] Here many participants who believed that they had efficiently blocked these practices, had in fact failed to configure the tool properly without noticing or misunderstood the intention of the configuration altogether.[640] In that sense, PIMS should be particularly careful in determining their interfaces in order to actually support the individual user.

Furthermore, what currently comprises a major practical hurdle in truly improving consent fatigue is arguably the requirement for consent to be specific. As discussed earlier (see Part 1 Chapter 2: C. I. 2. Specific), based on this prerequisite there is still a need to collect specific consent for each processing activity of each separate controller, as any sort of generalisations are essentially forbidden. [641] This also prevents any efforts for a more automated, technology-based form of consent management. Many platforms would certainly

---

[636] *Calo,* 82 Geo. Wash. L. Rev. 2014, 995, 1014; *Hermstrüwer*, 8 JIPITEC 2017, 9, para 36; *Hacker*, Datenprivatrecht, 618; *Ruschemeier*, in: KI, Demokratie und Privatheit, 211, 224.

[637] *Calo,* 82 Geo. Wash. L. Rev. 2014, 995, 1021.

[638] *Hacker*, Datenprivatrecht, 618.

[639] *Leon and others*, in: CHI '12, 589, 597f.

[640] *Leon and others*, in: CHI '12, 589, 595.

[641] *Voigt/von dem Bussche*, GDPR, 96; *Piltz*, 9 K&R 2016, 557, 563; *Gierschmann*, 2 ZD 2016, 51, 54; *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 68.

possess the technical means to simply execute the user's preferences for all websites automatically. This form of consent management is, however, rejected as incompliant with the consent requirements under the GDPR by many scholars. [642] Yet, as has been discussed previously, such a restrictive reading of the Regulation essentially contradicts both its purpose, as well as the user's interests (see Part 1 Chapter 2: C. I. 2. Specific). Furthermore, considering the effects of consent fatigue, holding onto this stipulation does not result in a higher level of privacy as individuals will effectively still simply "click away" any notice they encounter. The possibility of "bundling" the individual's preferences and executing them automatically in a technology-based manner is, after all, essential in order to truly improve the current state of consent.[643] A personalised, technological approach is also necessary in order to counteract the specific challenges arising from the new forms of personalised marketing and nudging, according to the individual's profile.[644] Based on that, a broader understating of the term should be supported. [645]

V. Intermin Conclusions: Consent

A number of Personal Information Management Systems offering a functionality of consent management have been developed in an attempt to solve the obstacles in the collection of truly valid consent, as outlined in this chapter. The achieved results can definitely be considered an important step in improving the current landscape in which consent and its prerequisites of freely given, unambiguous,

---

[642] *Hanloser*, 8 ZD 2023, 421, 421; *Schmitz*, 14 ZD-Aktuell 2023, 01304; Assion / *Aretz*, § 26 TTDSG, para 17; contrary opinion in: Geppert/Schütz / *Schmitz*, TTDSG §26, para 7-3; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 16.

[643] *Sattler*, Informationelle Privatautonomie, 383; *Hacker*, Datenprivatrecht, 620.

[644] *Calo,* 82 Geo. Wash. L. Rev. 2014, 995, 1021-1023; *Hacker*, Datenprivatrecht, 620.

[645] *Hanloser*, 8 ZD 2023, 421, 421; Assion / *Aretz*, § 26 TTDSG, para 17; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 16; *Hacker*, Datenprivatrecht, 619f.

specific and informed decisions, particularly in the online environment, can largely be described as an illusion. They are, however, as of writing, still subject to many limitations and are definitely far from the user-centric vision under which individuals would be given full and transparent control over the processing of their personal data, so often marketed by proponents of Personal Information Management Systems and consent management platforms, in particular. In addition to the current technical limitations of these tools, there is also a heated debate concerning the question of the legitimacy of consent, collected through PIMS in general. Many sources within literature point out that the requirement for consent precludes any level of generalisation on the side of the data subject, significantly limiting the practical benefits of such platforms. In the interest of both furthering Privacy Enhancing Technologies and supporting the right to informational self-determination, a broader understanding of "specific" consent should be supported. While the previously presented offerings are only examples of currently existing solutions, they do provide an accurate generalised overview of the options to date available on the market, including the existing limitations of such.

The solutions which can be considered most mature from a commercial perspective are World Data Exchange, MyDex, and Meeco. While the specific technical settings as well as the additional functionalities of all of these service offerings differ from one another, they do have one characteristic in common, which is particularly relevant in the context of considerations of PIMS: their functioning is largely dependent on the controller. Both World Data Exchange and MyDex can only be used by individuals for the management of their data flows and consent requests for the processing of personal data by businesses which have also signed up with the platform. As for Meeco, the platform might theoretically allow the set up of a digital-vault directly by an end user but this would require a substantive amount of technical knowledge and judging by the descriptions contained in the "Quickstart" guide, this was also not the intention. In that sense, the "user-centric" element of these PIMS is at least to a certain extent questionable, as these platforms will always have an underlying interest in continuing the cooperation with the businesses

conducting the requested processing activities, without which the offering would turn out to be empty. This limitation to certain controllers subscribing to the platform also means that data subjects are limited in the amount of data flows which can be managed. Therefore, they are also not in a position to allow full or comprehensive control over the processing of one's personal data but rather some control over certain processing activities.

A similar limitation applies to the application Plus Privacy created by the OPERANDO consortium. This is not dependent on the controllers, as no type of cooperation between those and the platform exists and the system actually does allow for the set up of privacy preferences, without making this dependent on the businesses in question. However, the limitation of the amount of data flows which can be managed is applicable. As of the time of writing, it was only possible for data subjects to configure their settings for the entirety of four platforms and while those are definitely to be considered key players (Google, Facebook, X and LinkedIn), the actual impact on the ability of the data subject to manage their processing operations is, in this context, more symbolic than significant. Also, as the project was closed in April 2018, new developments are not to be expected soon. This, however, shows a general problem: truly user-centric solutions which are not dependent on the controllers' cooperation are significantly harder and more expensive to develop, while being less likely to generate any significant proceeds. As a result, more innovative solutions focused on actually giving control to the individual are also underdeveloped, compared to the commercially more promising projects backed directly by large businesses.

The same applies to the last two examples: Advanced Data Protection Control and PRIVACY-AVARE. While both of these are rooted in innovative ideas and display an advanced approach to issues of data privacy, they are both still under development, with promising but still not fully functioning prototypes. In that sense, while they may in the future prove to allow a truly user-centric management of personal data flows by the data subject, this is not yet a reality, a fact which can be considered a limitation in itself.

D. Requests

Whereas the above sections focused on the possibilities in which PIMS could further the assurance of the general principles of data protection such as its security, integrity and confidentiality, as well as the transparency of processing operations, there are a number of prerogatives which are at least equally crucial in enabling the data subject to gain more control over their personal data. These are namely the rights to: access (Art. 15); rectification (Art. 16); erasure (Art. 17); restriction of processing (Art. 18); portability (Art. 20); and objection (Art. 21). These differ from the modalities discussed earlier in the sense that they generally do not require the controller to take action automatically but are rather based on the enquiries made by the data subject. This differentiation is also supported by the fact that Article 12 refers to the right under Articles 15–22 as "requests" of the data subject. Based on that, it makes sense to discuss these rights jointly, as many issues regarding the formalities and procedure of their assurance will apply equally to all of those.[646] The fact that their execution requires an action of the side of the data subject, in the form of a request made to the controller, also makes them particularly suitable for support through a Personal Information Management System. Individuals might not possess the necessary knowledge or tools to put forward such a request and since the realisation of their rights depends on it, providing them with guidance in this regard will have an immense effect of gaining of control over their personal data.

I. Universal Considerations

First of all, the general framework regulating the management of data subject requests needs to be considered. The following section

---

[646]Kuner and others / *Polčák*, Art. 12, 398, 406.

will therefore provide an overview of the common rules governing all data subject requests put forward in the GDPR, including questions of their form, timing, and cost, as well as exemptions from the requirement to facilitate such. While the involvement of a third-party provider might significantly further the practical use and relevance of those rights, there are also certain challenges that need to be considered. The efficient administration of data subject requests already possess difficulties in everyday company practice and the involvement of a third party adds a new level of complexity, as well as risks. These risks do not only materialise on the side of the controller, as the question of secure identification and safeguards for data transmission affect the data subject equally.[647] In this sense, these practical hurdles need to be carefully analysed in order to ensure that the rights and freedoms of the data subject are in fact protected accordingly. Equally, the ways in which the involvement of a PIMS could ease the exercise of the individual's rights will be considered.

1. Form and Format

The question of how information should be provided and by what means has already largely been answered in the context of the right to information under Part 1 Chapter 2: B. I. 1. and 3. At this point, a reminder that in accordance with Art. 12(1) any communication towards the data subject concerning the processing of their personal data should be conducted "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language".* The realisation of this goal is to a certain extent simpler than it was in the case of the general right to information, since in that case, the subject requests that the controller will be in active communication with the individual, allowing them to adjust elements such as language, complexity and level of detail provided in accordance to the specific circumstances. While thereby partly alleviating the problems caused by the conflict of objectives, the reply to a request in turn also creates a

---

[647]For an overview on multiple threat models refer to: *Pavur/Knerr*, GDPArrrrr, 1, 1ff.

need for specification, meaning that the provided information will have to specifically relate to the processing of the individual's personal data, whereas references to general data protection policies or terms of services would be unacceptable.[648]

In principle, the freedom of choice when it comes to the form of communication with the data subject outlined in Article 12 (*"information shall be provided in writing, or by other means, including, where appropriate, by electronic means"*) still applies. However, additionally to the limitations set out by the principle of accountability, as well as the requirements of transparency and intelligibility mentioned before, Article 12(3) adds another condition stating that *"[w]here the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject".* While only electronic means are explicitly mentioned herein, the basic principle of continuing communication with the data subject through the same channel via which a request has been received, should generally be extended to all other mediums.[649] This does not mean that the data subject would have the right to dictate the form of communication as there might be circumstances in which the selected channel is either impractical, insecure or inadequate for other reasons.[650] It implies, however, that in consideration of the relevant circumstances, the controller should take the wishes and reasonable expectations of the data subject into account.[651]

Interesting in that context is the question to what extent the controller would actually be required to answer data subjects' requests, submitted over a Personal Information Management System or other

---

[648]Sydow/Marsch / *Greve*, Art. 12, para 19.

[649]Kühling/Buchner / *Bäcker*, Art. 12, para 17; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 35; Sydow/Marsch / *Greve*, Art. 12, para 25.

[650]The controller might for example insist on contacting the person over the usual channel of communication, if a request is received through new means and there are doubts about the individual's identity. For more information on the question of identity checks refer to Part 1 Chapter 2: D. I. 3. Identification.

[651]Kühling/Buchner / *Bäcker*, Art. 12, para 1; *EDPB*, Guidelines 01/2022, para 128.

intermediary, through that third party as well, or if the data subject could instead be contacted directly. The European Data Protection Board does comment on that issue, stating that the controller is not per definition obliged to provide the requested information to the portal.[652] As an example, the Board describes a scenario in which the controller would be aware of security issues being insufficient on the side of the intermediary.[653] While helpful this, however, does raise additional questions. First of all, would the same apply in circumstances in which the data subject, aware of the security gaps, still wish to have their requests answered in that way? Secondly, could the controller refuse to deal with a request over a third-party portal, based on arguments other than the interest of the data subject? As for the first question, unless the data-set also contained the information of other individuals whose rights and freedoms might be endangered or sensitive company data requiring protection, there seems to be no reason not to act in accordance with the data subject's wishes. This would, after all, be in the interest of the natural person's digital self-determination, as it allows them to make a decision on how their information should be handled.

Regarding the second question, the provision of a clear answer is significantly more difficult as multiple aspects need to be taken into consideration. A simple refusal based on minor inconveniences or organisational difficulties will most likely not suffice if the data subject asks for communication to take place through the selected platform or intermediary. Article 12 clearly creates an obligation for the controller to use easily accessible forms and the personally chosen channel will logically be the most convenient for the individual. If, on the other hand, legitimate reasons existed which would preclude the controller from submitting information through the PIMS, these should also be weighed accordingly against the data subject's interests. Both the right to obtain a copy (Art. 15(4)) and to data portability (Art. 20(4)), for example, contain a restriction stating that the corresponding right shall not adversely affect the rights and freedoms of

---

[652] *EDPB*, Guidelines 01/2022, para 90.
[653] ibid 89.

others. This also explicitly does not solely refer to the data protection rights of other individuals but according to Recital 63, also covers information such as trade secrets, intellectual property or copyright protecting the software. If these types of interests were therefore at a higher risk in case of a submission of data through the PIMS provider, a weighing of interests would be required, examining possible alternatives.[654] Where the controller could demonstrate the capability of offering means able to secure a higher level of protection for those rights without unnecessary impediments for the data subject, information might need to be provided though another channel instead of the Personal Information Management System.[655] A similar restriction is also imaginable if the submission via the PIMS made it impossible for the controller to document the process and therefore comply with the principle of accountability in accordance with Art. 5(2). Under those circumstances, the use of alternative means of communication could prove to be necessary.

2. Facilitation

Another element which needs to be taken into account is the original purpose lying behind the engagement of the PIMS provider. In most instances, this will be precisely for the reason that data subjects do not want to deal with the management of such requests in a traditional way. For example, the PIMS might allow them to put forward requests to multiple controllers. If the individual had to monitor multiple channels of communication in order to handle those, this would require a substantial amount of effort, whereas the management through one system can be considered more efficient. Moreover, a

---

[654]Gola/Heckmann / *Franck*, Art. 15 DSGVO, para 49; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 14 DSGVO, para 17; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 35.

[655]For example, the controller might be open to submitting redacted versions of certain documents though the PIMS, but only offer on-site access to the original sources. The same might also apply where the controller needs to insist on particular encryption techniques, required for the protection of company data, not supported by the PIMS provider.

person might be unwilling to deal with the controller at all, engaging a provider specifically to take over the administration on their behalf.[656]

The purpose of utilising the PIMS is important in the context of the requirement of facilitation put on the controller. Article 12(2) GDPR states that companies *"shall facilitate the exercise of data subject rights under Articles 15 to 22"*. Stemming from this regulation are two distinct responsibilities. First of all, the controllers have to establish appropriate channels of communication through which individuals can contact them and put forward their requests.[657] Secondly, they should refrain from the creation of any obstacles or demands that might hinder the data subject from the exercise of their rights.[658] In that sense, the refusal of the controller to provide answers or continue communication via the Personal Information Management System could be seen as such an obstacle. Where the utilisation of the PIMS enables the individual to act upon their rights, the inability to do so will logically have the potential to hinder them. To this end, the general presumption should be that the controller would in fact be required to act upon requests through a system preferred by the data subject, whereas a very strict standard would have to apply for any contrary company interests.

3. Identification

Another issue frequently arising in the context of data subject requests in general relates to the question of identification.[659] This aspect has two separate dimensions. The first defect in identifiability

---

[656]This for example works fairly well in the case of deletion requests, where the data subject is not necessarily interested in any details regarding the processing, but simply want their information removed.

[657]Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 14; Kühling/Buchner / *Bäcker*, Art. 12, para 25.

[658]Kuner and others / *Polčák*, Art. 12, 398, 410; Eßer/Kramer/von Lewinski / *Eßer*, Art. 12 DSGVO, para 20; Sydow/Marsch / *Greve*, Art. 12, para 22.

[659]*Raji*, 6 ZD 2020, 279, 280ff; *Dausend*, 3 ZD 2019, 103, 104; *Piltz*, 10 K&R 2016, 629, 629.

occurs where it is clear by whom a request is made but the controller is, however, unable to locate the corresponding dataset in their systems.[660] The second applies in instances where it is clear which person and corresponding information the request refers to but where the controller has doubts regarding the identity of the requesting individual.[661] Additionally, the involvement of a third party creates questions regarding the verification of such. While not explicitly mentioned in the GDPR, these will become highly relevant in the context of Personal Information Management Systems and should therefore be considered as well.

a) Identification of a Link

In general, Article 12(2) of the GDPR stipulates that companies are not required to comply with data subject requests if they are unable to identify the individual. This inability should, however, not be read as simply referring to difficulties or hindrances in identification. It is clear that technical and organisational measures such as pseudonymisation, data segregation, encryption, and access restrictions will make finding all relevant information, which will possibly be scattered throughout multiple systems, significantly more difficult.[662] In the line of the requirement of facilitation, these difficulties should, however, be taken into account while initially planning the processes for compliance with such a request.[663] In that sense, the controller is required to use all available resources to allow identification.[664] Article 12(2) also asks for the controller to *"demonstrate"* such an inability. In connection with the general principle of accountability, this

---

[660]Kühling/Buchner / *Bäcker*, Art. 12, para 29; Sydow/Marsch / *Greve*, Art. 12, para 23.

[661]Kühling/Buchner / *Bäcker*, Art. 12, para 30; Sydow/Marsch / *Greve*, Art. 12, para 30.

[662]*Veale/Binns/Ausloos*, 8 IDPLaw 2018, 105, 115-117.

[663]*Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 11, para 5; Kühling/Buchner / *Weichert*, Art. 11, para 11af.

[664]Gola/Heckmann / *Gola*, Art. 11 DSGVO, para 3; Kühling/Buchner / *Weichert*, Art. 11, para 13.

should be understood as an obligation to document the actions taken to enable the detection of the data, as well as the reasons behind the impossibility to do so accordingly.[665]

However, Article 11(1) also clearly stipulates that there is no obligation on the side of the controller to further maintain, process or additionally acquire any personal information for the sole purpose of complying with the regulation in general, including data subject requests. The same is also supported by Recital 64, stating that the *"controller should not retain personal data for the sole purpose of being able to react to potential requests".* This specification has been made in order not to undermine the principles of data minimisation and storage limitation, as otherwise businesses might be inclined to further store large amounts of directly identifiable information simply for the purpose of answering any possible future request by the individual.[666] On the other hand, individuals are given the option to voluntarily provide additional information enabling their identification in accordance with Art. 11(2).[667] In that case, the controller would again be required to act upon such a request.[668]

b) Identification of the Data Subject

The second potential defect in identifiability refers to instances in which the controller has doubts as to whether or not the person making the request is, in fact, the data subject. It is clearly necessary for the controller to ensure that the request they are looking to comply

---

[665]*Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 11, para 29; Eßer/Kramer/von Lewinski / *Eßer*, Art. 11 DSGVO, para 13.

[666]*Hansen* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 11, para 2-4.

[667]This might for example be the case, where the controller has effectively pseudonymised a certain dataset, making it impossible to link it to a natural person based on a clear name. If, however, the data subject, submitted the pseudonym or other data contained in the set (for example a unique combination of age, gender and blood type) the controller would be enabled to link the data to the individual.

[668]Gola/Heckmann / *Gola*, Art. 11 DSGVO, para 13; Eßer/Kramer/von Lewinski / *Eßer*, Art. 11 DSGVO, para 19.

with is coming from such, as submitting details of the processing activities, erasing information, or providing copies of personal data to an unauthorised body would constitute a breach in the meaning of Art. 4 No. 12 GDPR. Also, acting on any of those rights without the data subject's knowledge could pose a serious threat to the individual's rights and freedoms, which is why any such instances are to be treated with extreme caution.[669] This concern will be of particular relevance for the submission of a data subject request through a Personal Information Management System. Since the request will most likely be submitted using a channel other than the usual form of communication with the individual (such as user accounts, e-mail, or other) and since the controller might not even be in direct communication with the individual at all (if a third-party provider took over the handling of the request, for example) it might not be uncommon for businesses to be concerned about the validity of such request. Adding to that initial difficulty is the fact that while controllers will often already have appropriate identification procedures in place for their customers, they could be unable to use those for requests submitted via another system, namely the PIMS, furthering the complications with the verification of the data subject's identity.[670]

For such instances Art. 12(6) allows businesses to request the provision of additional information necessary for the confirmation of the individual's identity. While definitely an important prerogative for any business struggling with suspicions regarding a specific request, there are a number of aspects that need to be taken into account

---

[669] *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 37, supports the notion that the controllers' rights listed in Article 12(6) may convert into a legal obligation to confirm the individual's identity, where serious doubts regarding such emerge.

[670] For example, businesses often embed the possibility of submitting a DSR in the privacy dashboard of the user account. In order to access such, the individual will, however, already have had logged into the account, thereby completing the authentication procedure of the controller. In that case, there are rarely grounds for doubting the person's identity. If, however, the same request was submitted though a portal, simply requesting to delete, adjust or transfer data from a particular account, the controller would need to insist on another form of verification.

when applying it. First of all, since the collection of additional data points for the purposes of verification also constitutes a processing activity, all general requirements of the GDPR apply to the same extent. This means that, in accordance with the principle of data minimisation, the requested information should be adequate, relevant, and limited to what is necessary in order to confirm the individual's identity.[671] In that sense, any excessive or precautionary accumulation of evidence is strictly prohibited.[672] Further processing of the collected information is also not allowed, based on the principle of purpose limitation.[673] In consideration of the general requirement of facilitation imposed on each controller under Article 12(2), the application of any sort of identification procedures which might put a significant burden on the individual and thereby impede such from exercising their rights would also be invalid.[674]

Based on the many aspects and opposing interests requiring consideration, the European Data Protection Board recommends the administration of a proportionality assessment, taking into consideration all relevant elements, including the context of the request, its content, the type of data affected and any potential risks which might result from an improper disclosure.[675] This flexible approach to the selection of the specific means of identification is also supported by Recital 64 which clarifies that controllers should *"use all reasonable measures"* for the verification of the data subject's identity. In light of that, companies are generally urged to base their verification procedures on information already available to them, rather than collecting

---

[671] Sydow/Marsch / *Greve*, Art. 12, para 30.

[672] *EDPB*, Guidelines 01/2022, para 68.

[673] *Petrlic*, 43 DuD 2019, 71, 72 and 74; Eßer/Kramer/von Lewinski / *Eßer*, Art. 12 DSGVO, para 38; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 37.

[674] *EDPB*, Guidelines 01/2022, para 71; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 36.

[675] *EDPB*, Guidelines 01/2022, para 70.

vast amounts of new data.[676] Highly debated in that context is, for example, the validity of requesting identity cards.[677]

Such a proportionality assessment might, however, lead to a quite controversial outcome in the context of Personal Information Management Systems. If, for example, the submitted request concerned high-risk processing operations or the disclosure of sensitive personal information, the controller might see it as necessary to insist upon a secure verification procedure and the confirmation on multiple details before proceeding with the request. Such a procedure could both require the provision of additional information and, due to its length or complication, make the exercising of the data subject's rights more difficult. Where the controller already has appropriate identification channels put in place as part of their user account verification or similar system, the outcome of the proportionality assessment might thereby indicate that the use of these would be the more proportionate and data protection friendly option. In that case, the assessment of proportionality would indirectly require the controller to insist upon the use of their channel, rather than the PIMS. This would in a sense undermine the whole purpose of using the Personal Information Management System as an intermediary in the first place, as the individual will in most instances have engaged such precisely for the reason of not wanting to manage their request over the traditional channels.

It could be argued that the decision regarding the form of communication should be made by the data subject, since they would be the ones bearing the consequences resulting as part of the extended verification procedure. This, however, is only true to a certain extent. If the controller had to, in accordance with Art. 12(2), request the provision of additional information directly confirming the identity of

---

[676] *Singh/Cobbe*, 17 IEEE S&P 2019, 21, 24; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 37; *EDPB*, Guidelines 01/2022, para 73; Sydow/Marsch / *Greve*, Art. 12, para 30.

[677] *Raji*, 6 ZD 2020, 279, 281ff; *Petrlic*, 43 DuD 2019, 71, 72f; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 36; Eßer/Kramer/von Lewinski / *Eßer*, Art. 11 DSGVO, para 38; *EDPB*, Guidelines 01/2022, para 75.

the natural person in order to comply with the request submitted through the PIMS, this would result in the establishment of a new processing activity. As already mentioned, all the rules governing such would thereby apply to the same extent. The controller would, as a consequence, need to assure the secure handling of such data and its timely deletion, potentially deal with and notify breaches where applicable, consider the process in its record of processing activities, and make sure all is documented in line with the principle of accountability. This does not only constitute a significant burden but is also a serious liability. In that sense, the controller might have an interest in insisting upon the verification over the existing channels, rather than alternative methods. Should that be the case, the outcome will be a completely absurd scenario, in which the data subject would verify their identity over the channels already in place on the side of the controller in order to receive an answer through the PIMS, potentially leading that person to question the actual advantages of engaging the intermediary in the first place. In consideration of this dilemma, it would be highly advisable for developers of Personal Information Management Systems to take these issues into account and embed appropriate identification procedures compatible with those of other service providers within their functionalities.

c) Verification of Third Parties

Apart from potential problems regarding the identification of the data subject, another hurdle emerging as a consequence of exercising data subject rights through a third-party provider is the question of the verification of the portal itself. While theoretically the idea behind a Personal Information Management System is the facilitation of more control on the side of the data subject and the most complete protection of that individual's data, no certification or other form of attestation legitimacy of such providers exists at the moment. Based on that, controllers receiving requests through such portals will inevitably be required to verify the legitimacy of these requests in order to avoid disclosing information to unauthorised parties, thereby causing a breach.

The EDPB points out that national laws governing legal representation would also need to be taken into account, to the extent that they might impose specific requirements for demonstrating authorisation to manage requests on behalf of a natural person.[678] This might be especially burdensome for small and medium businesses receiving such requests from PIMS providers located within other jurisdictions, as they would first need to enquire as to the respective national laws and practices, potentially in a foreign language. Furthermore, the existence of a legal authorisation on the side of the PIMS would again need to be documented by the controller in accordance with the principle of accountability.[679] While such practical obstacles in handling requests do not pose a ground for refusal to act on such (see more under Part 1 Chapter 2: D. I. 6. Exemptions), they might under certain circumstances be considered sufficient for a deadline extension under Art. 12(3) (see more under Part 1 Chapter 2: D. I. 4. Timing).

What should also be contemplated at this point is that the here listed requirements regarding the verification of the PIMS apply based on the assumption that the portal is to be considered a third party. As per Article 4 No. 10 this "*means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data"*. The European Data Protection Board certainly seems to support this designation in their Guidance on the right to access.[680] This, however, is not the assumption lying at the heart of this thesis. Detailed considerations on the legal classification and role taken towards the data

---

[678]*EDPB*, Guidelines 01/2022, para 79.

[679]ibid para 79.

[680]ibid para 88: "*There are companies that provide services which enable data subjects to make access requests through a portal. The data subject signs in and gets access to a portal through which they can submit for example an access request, request data rectification or data erasure from different controllers. Different questions arise from the use of portals provided for by a third party*."

subject will be contained in the second part of this paper. The question of the status of the PIMS will therefore be left open at this point. It should, however, be noted that where a different legal designation might be given to the Personal Information Management System, the responsibilities will change accordingly. In the case of obtaining the status of a processor or controller (joint or otherwise), the described verification would most likely solely take place in the form of a pre-contractual measure and the extent of the liability of the company receiving the request might be substantially limited.

4. Timing

In accordance with Article 12(3), information on any action taken on a request should be provided to the data subject without undue delay and in any event, at the latest within one month after the request has been received. Where the controller is unable to comply with the request within the defined time-frame, due to the amount or complexity of such, the deadline can be extended by another two months. This extension, however, needs to be communicated to the data subject within the before mentioned one month deadline. In that sense, the data subject has a right to receive, within one month, information regarding either (1) the compliance with the request; (2) the extension of the deadline; or (3) the refusal to act based on Art. 12(5)(b).[681]

Based on the use of the conjunction “and”, some voices in literature support the view that the conditions for extending the one month deadline should apply cumulatively.[682] Others, on the other hand, argue that the presence of each of these elements on their own could potentially cause an inability to comply within one month and that

---

[681]Kuner and others / *Polčák*, Art. 12, 398, 409.

[682]Kühling/Buchner / *Bäcker*, Art. 12, para 34; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 33.

such a restrictive interpretation could therefore not have been intended by the lawmakers.[683] The second view should be followed for multiple reasons. First of all, an alternative understanding of the two conditions would not automatically lead to regular extensions by larger enterprises based on the amount of requests,[684] since they are still subject to the facilitation requirement under Art. 12(2). The possibility of extension therefore does not cover instances of routinely receiving numerous requests as in such a case, the controller would be obliged to create appropriate capacities to deal with those.[685] In the event an unproportionally large amount of requests was to be submitted unexpectedly at a certain time, the granting of an extension could, however, still be reasonable,[686] even for large enterprises.[687] Another reason why the conditions of Art. 12(3) should be considered as an alternative is that while the conjunction "and" is used, it solely refers to taking into account both elements, which does not equate to the fact that both elements have to be present. For example, a request might be more complex than the usual ones a controller receives but could still be complied with within one month through the use of additional resources. If, on the other hand, a controller received multiples of such "medium complexity" requests at a time, the combination of the two might lead to an inability to fulfil all requests on time. In the same vain, one single request might, however, encompass such a high level of complexity that a longer period would be required for its handling. Such an understanding, in which all elements are taken into consideration and a determination as of

---

[683]Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Schneider,* 'Art. 12' DSGVO, para 52; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 25.

[684]This view has been presented in: Kühling/Buchner / *Bäcker*, Art. 12, para 34; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 33.

[685]*EDPB*, Guidelines 01/2022, para 162: *"If controllers often find themselves forced to extend the time limit, it could be an indication of a need to further develop their general procedures to handle requests.*"

[686]*EDPB*, Guidelines 01/2022, para 164.

[687]If for example interest groups organised a large campaign to submit mass data subject requests in order to disrupt its business.

the necessity of an extension is made based on the specific circumstances of the case, would also be in line with the general adaptability endorsed by the GDPR.

In the context of data subject requests received through Personal Information Management Systems, the question of timely compliance can become quite relevant. As outlined above, controllers might on a regular basis face difficulties in properly identifying the data subject, as well as verifying the validity of the portal and its security level. Should such doubts arise, communication with the provider and the individual might need to take place, further prolonging the process. In this context, the question arises as to what extent an extension of the one-month period might be warranted. The EDPB refers to a suspension in time, rather than an actual extension in that context, suggesting that such a suspension would apply until the controller has obtained the necessary information from the data subject.[688] Conversely, difficulties in the identification or verification of the parties involved in the request would, however, not automatically amount to the designation as a "complex" request. This would also be supported by the fact that data subject requests submitted via third-party providers will most likely increase over time and potentially become the norm, creating the obligation for controllers to put in place appropriate procedures for their effective and efficient handling.

5. Costs

Article 12(5) demands that all actions and communications taken in order to comply with a request of a data subject should be free of charge. This is in line with the general requirement to facilitate such requests, as potential expenses incurred by the data subjects might hinder them from acting upon their rights at all. In consideration of the central importance of the data subject right for the protection of their personal data, it would also be highly problematic if the exercise of such could be made dependent upon a payment of a fee.

---

[688] *EDPB*, Guidelines 01/2022, para 159.

This rule, however, solely applies to the data controller and not to the provider of the PIMS. These are therefore free to charge for their provided services, to the extent that they facilitate data subject requests on processing activities of other businesses. If, on the other hand, an individual submitted a request to the PIMS regarding their processing of personal data, no compensation could be requested for that. Data subjects would also be unable to transfer the expenses incurred as a result of using a PIMS onto the controller, since the prevailing opinion assumes that individuals have to cover their own costs of submitting a request, such as postal charges, cost of paper, cost of printing out copies etc.[689] If, on the other hand, the controller failed to establish appropriate channels for data subjects to exercise their rights or refused to act upon such, thereby infringing the Regulation, and the data subject had to engage the PIMS in order to exercise their rights, it might be possible for the individual to claim damages under Art. 82.[690]

6. Exemptions

Article 12(5) provides for two exemptions under which controllers would be able to refuse complying with a request or alternatively charge a fee. This is the case in which a data subject request is deemed to be manifestly unfounded or excessive. The Article already recognises the most prevalent reason for excessiveness, which is the "repetitive character" of such requests. While the regulation does not give any specific limit as to the amount of requests an individual can submit within a certain time frame, some Member States have enacted such limitations, with the most common one being one request per year.[691] While these are certainly helpful in providing a general guidance for controllers, they should not be applied too literally,

---

[689]Eßer/Kramer/von Lewinski / *Eßer*, Art. 12 DSGVO, para 34; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 42.

[690]No such case has been brought to the courts yet, but damages for providing delayed or incorrect information have for example been awarded in: LAG Niedersachsen, ZD 2022, 61and OLG Köln, DStRE 2023, 571.

[691]Kuner and others / *Polčák*, Art. 12, 398, 408.

as there might be instances where more frequent submissions are in fact justified.[692] This could, for example, be the case for processing activities which are regularly subject to modifications or in situations where the circumstances surrounding such have recently changed, either on the side of the data subject (new reason for objection) or legally (transfer mechanism declared void). Where, on the other hand, frequent submissions of requests containing the exact same content occur, excessiveness can be affirmed.[693]

Manifestly unfounded requests constitute a rare exception in the everyday business practice.[694] Theoretically, these might occur if one is submitted by a person obviously unrelated to the data subject or where the factual preconditions for a certain right are evidently not present.[695] Since. However. data subjects are not required to provide any reason for their request, it is usually difficult, if not impossible, to prove their lack of justification, especially on first glance.[696] Even in the case of unclear motives or wrongly cited legal basis, the general requirement to facilitate would oblige the controller to further enquire as the wishes of the individual.[697] Also “precautionary” requests, in which the individual does not necessarily suspect that any processing would take place, but simply wants to find out in case there are any activities, lie well within the individual’s rights and cannot be automatically classified as unfounded.[698] Furthermore, their lack of practical applicability is largely based on the fact that the controller would need to “demonstrate” the excessive or unfounded character

---

[692] *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 33; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 43.

[693] Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 43; Eßer/Kramer/von Lewinski / *Eßer*, Art. 12 DSGVO, para 35.

[694] Eßer/Kramer/von Lewinski / *Eßer*, Art. 12 DSGVO, para 35.

[695] Gola/Heckmann / *Franck*, Art. 12 DSGVO, para 33; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 32.

[696] Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 43.

[697] *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 32.

[698] Kühling/Buchner / *Bäcker*, Art. 12, para 37.

of the request.[699] In many instances, it will therefore simply be more practical for controllers to send out a standard reply, confirming that no data of the individual is being processed, rather than start an investigation into its level of substantiation.[700]

Controllers might, however, be more inclined to take on the administrative effort of disputing requests if they start to receive such on a larger scale from one provider. While some PIMS offering functionalities supporting the handling of data subject requests require the data subject to identify the controller individually, or perform some sort of analysis of providers who actually possess personal data on a specific natural person,[701] others for example present a pre-formulated list of businesses from which the person can request deletion or access.[702] Users of such platforms might, however, be inclined to simply select all of the listed companies, either on a precautionary basis or simply to avoid the hassle of verifying these separately. As a result, mass requests are being sent out to various companies, without ever establishing a link between the data subject and the controller.[703] In such instances, especially once a controller submitted negative replies on a number of those, the question might

---

[699]Kuner and others / *Polčák*, Art. 12, 398, 408; *EDPB*, Guidelines 3/2019, para 98.

[700]Kühling/Buchner / *Bäcker*, Art. 12, para 37.

[701]For example, Revoke apparently used to perform an analysis of where personal data of individuals can be found before offering to submit a request on their behalf. As of September 2022 the page staed: *"Revoke helps you identify companies that hold your personal data. We do this through our Dark Web Search, Privacy Checks, and Mailbox Search features. We never contact a company on your behalf without your explicit permission"*, https://revoke.com/privacy-policy-european/ (accessed: 05 September 2022). This statement can however no longer be found on their webpage.

[702]For example, Privacy Bee built a database of companies. These are visible in the user dashboard, from which individuals can select businesses for opt-outs. The portal then submits those requests on behalf of the user. See FAQ Question *"How does Privacy Bee work?"*, https://privacybee.com/faq/ (accessed: 11 October 2025).

[703]https://iapp.org/news/a/why-some-dsr-services-create-compliance-concerns/ (accessed: 22 February 2026).

arise as to whether or not these could, in fact, be considered excessive or manifestly unfounded. After all, a company would have collected a whole catalogue of unsubstantiated requests by then, supporting such a claim. This line of argumentation will, however, not hold based on the very fundamental and individual character of data subject rights. The controller has to be able to demonstrate the lack of foundation or excessiveness of a specific request, coming from a specific data subject. Since this will be almost impossible as it cannot be ruled out that one of the submitted DSR is in fact credible, controllers will most likely have to continue complying with such, unless there are other grounds for rejection (for example, doubts regarding the identity of the data subject as outlined under Part 1 Chapter 2: D. I. 3. Identification). Interesting in that context would be, however, the possibility of exploring an analogous right to charging a fee from the PIMS provider based on Art. 12(5)(a).

7. Restrictions

Article 23(1) contains an opening clause for Member States to put in place laws restricting the individual's data subject rights where this is necessary for the protection of other goods such as national security, defence, judicial independence, or the prevention, investigation, detection or prosecution of criminal offences. This is in line with the general understanding that data protection, while certainly being a fundamental right, is not absolute and may therefore be restricted in consideration of other legitimate interests of the democratic society where necessary and proportional.[704] Where such restrictions exist, controllers would clearly not be required to comply with the request.

II. Specific Considerations

Whereas the above section has outlined the requirements and corresponding considerations in the context of PIMS universal for all types of data subject requests, as a next step the specific rules governing each type should be analysed. The rights to access (Art. 15),

---

[704]Kuner and others / *Moore*, Art. 23, 543, 550.

rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18), portability (Art. 20), and objection (Art. 21) all have unique characteristics which will present themselves in various functionalities of Personal Information Management Systems. To that extent, their particular potentials as well as associated challenges should be discussed below.

1. Access

While Article 15 of the GDPR is entitled "right to access by the data subject", the clause actually contains four independent components. The first two are the separate rights to obtain a confirmation of and details about the processing. Also, additionally to being able to request direct access to the data, individuals can ask for a copy of such to be provided to them.

a) Confirmation

In accordance with the first sentence of Article 15, each individual has the right to obtain a *"confirmation as to whether or not personal data concerning him or her are being processed"*.

aa) Precautionary Request

This directly supports the validity of precautionary requests mentioned under Part 1 Chapter 2: D. I. 6. Exemptions, as the clause clearly recognises the possibility of answering requests where no personal data about an individual is being processed. While some consider that such an individual would no longer fall under the definition of "data subject",[705] the GDPR still clearly requires the provision of a negative declaration regarding the lack of processing of such a natural person.[706] This will include both scenarios where processing of personal data has never occurred or where it has been

---

[705]Gola/Heckmann / *Franck*, Art. 15 DSGVO, para 6.

[706]Kuner and others / *Zanfir-Fortuna*, Art. 14, 434, 462; *DSK,* Kurzpapier Nr. 6, 1; *EDPB*, Guidelines 01/2022, para 18.

already deleted or anonymised.[707] In that sense, the relevance of such a confirmation should not be underestimated as it can, to an extent, fulfil the function of auditing the controller's compliance with the regulation, where, for example, an individual is aware that his or her data has been processed and is seeking to verify that this is no longer the case. From this perspective, the right to confirmation can definitely be viewed as separate from the other elements of Art. 15, as it can be granted independently.

bb) Pre-Confirmation

In the context of Personal Information Management Systems, the right to confirmation is the least likely to cause any complications due to its rather uncontroversial content. Additionally, in instances where a request for confirmation or access would be submitted via the PIMS, there are also tools which offer a kind of "confirmation functionality" independently from the right to access or in combination with other rights. The tools Revoke,[708] DeleteMe,[709] or Mine,[710] for example, are mainly focused on the facilitation of deletion requests and the exercise of the right to object but will, depending on the specific offering, as a first step perform searches on the client's mailbox, the dark web, or various databases identifying where the client's personal data is being held. To which extent these analyses are actually accurate or are more of a guess is unclear but they can definitely be considered as a kind of "pre-confirmation" guiding the data subject toward potential processing activities.[711]

---

[707]Ehmann/Selmayr, *Ehmann*, Art. 15, para 29.

[708]Revoke, https://revoke.com/ (accessed: 22 October 2025).

[709]DeleteMe, https://joindeleteme.com/ (accessed 22 October 2025).

[710]Mine, https://www.saymine.com/ (accessed 22 October 2025).

[711]The concept of functionalities not facilitating the exercising of a right directly, but providing the user with the necessary information to target their requests is also acknowledged in: *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 12.

b) Details

Where a controller has confirmed the processing of personal data towards a data subject, or where that person is already aware of the existence of such, the individual can demand to receive detailed information regarding the processing activity in question.

aa) Relationship with the Right to Information

A long list of relevant facts to be submitted to the data subject on demand is contained in Article 15 (1) and (2) and includes more or less similar elements to those outlined in the context of the right to information under Articles 13 and 14. It should, however, be noted that those are in fact separate rights and that simply referencing existing privacy policies cannot be regarded as a facilitation of the individual's rights under Art. 15.[712] The provided details should directly relate to the specific processing of personal data of the individual in question. Whereas generalisations and abbreviations might be necessary in the interest of providing concise and transparent information to the general public, an overview submitted directly to the concerned individual should be specifically tailored to that person, as well as far more precise and granular.[713]

bb) Practical Execution

In practice, this is probably one of the rights most frequently taken advantage of by individuals and has been exercised quite often, in particular immediately after the GDPR came into force.[714] This might be due to its relatively easy execution on the side of the data subject.

---

[712]According to the Guidelines of the European Data Protection Board, the text might be based on the controller's privacy notice or record of processing activities, but would need to be tailored to the specific request. See: *EDPB*, Guidelines 01/2022, para 20.

[713]Kuner and others / *Zanfir-Fortuna*, Art. 14, 434, 462.

[714]https://www.forensicrisk.com/news-and-insights/the-rise-and-rise-of-data-subject-access-requests-dsars (accessed: 07 March 2026); https://www.hrmagazine.co.uk/content/news/rise-in-data-requests-costing-businesses-millions/ (accessed 25 February 2026).

Based on the requirement of facilitation, controllers must monitor all incoming channels for such requests. Therefore, it is sufficient for the data subject to send a standardised text through any e-mail or contact form and see what happens. A quick Google search also evidences a large array of such pre-formulated templates, from legal firms,[715] Data Protection Authorities,[716] consumer associations,[717] and others[718] which only require a minimal level of customisation on the side of the individual. Data access requests have also significantly impacted businesses, with three out of four small and medium enterprises reporting that their business had undergone changes to comply with Articles 15 and 16 of the GDPR.[719] Still, studies seem to indicate that these are not being handled to customers' satisfaction or in accordance with the legal requirements. Individuals generally consider their experience with access requests to be negative in terms of empowerment and transparency.[720] This subjective feeling seems to be supported by the objective facts. A review conducted into subject data access in the context of advertising found that over 58% of the companies failed to respond within the required 30 days, whereas only one actually provided a notification on the extension of

---

[715]Hensche Rechtsanwälte, https://www.hensche.de/musterschreiben-auskunftsverlangen-des-arbeitnehmers-gemaess-art-15-ds-gvo.html (accessed: 16 October 2025); Anwaltskanzlei Harzewski, https://rechtsanwalt-harzewski.de/auskunft-nach-art-15-dsgvo/ (accessed: 16 October 2025).

[716]https://www.baden-wuerttemberg.datenschutz.de/muster-auskunftsanspruch-nach-art-15-ds-gvo/ (accessed: 16 October 2025).

[717]Verbraucherzentrale, https://www.verbraucherzentrale.de/sites/default/files/2019-10/Auskunft_nach_Art._15_DSGVO.pdf (accessed: 16 October 2025).

[718]See for example: Generator für Auskunftsersuchen, https://datenschmutz.de/auskunft (accessed: 22 October 2025); Datenfragen, https://www.datenanfragen.de/blog/musterbrief-dsgvo-anfrage-auskunft/ (accessed: 22 October 2025); Heise Online, https://www.heise.de/news-ticker/meldung/DSGVO-So-nutzen-Sie-Ihre-Auskunftsrechte-4429886.html (accessed 22 October 2025).

[719]*Thibault*, Evaluating the Impact, 15.

[720]*Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 15.

the deadline.[721] Prior to actually receiving an answer, individuals *often* had to overcome a number of administrative hurdles, including long e-mail exchanges, the provisions of an ID, or signing affidavits without ever referencing any reasonable doubt by the companies.[722] Another typical hindrance leading data subjects to a feeling of frustration, is the practice of referring to the privacy policy.[723] This combination of obstacles can *often* create the impression of having to "jump through hoops" in order to receive the desired information. Exacerbating this situation even more is the fact that responses are also largely incomplete, thereby adding to the general dissatisfaction.[724]

These issues with the provision of the necessary details are, however, not only based in the controller's unwillingness to respond to the request of the data subject but also result largely from the inherent conflict between the requirements of erasure, confidentiality, pseudonymisation, roles and rights concepts, and many other elements which are part of the general technical and organisational measures, as well as the principle of data protection by design and default.[725] On the one hand, controllers are required to keep all personal data in a form making direct identification as difficult as possible and separate from any data serving a different purpose; on the other hand, however, they also have to be able to ad hoc locate all relevant information and provide a detailed report on its processing. This unfortunately is a general hurdle, in a sense, directly built-into the framework of the GDPR that Personal Information Management Systems are unlikely to overcome.

---

[721] *Urban and others*, in: Data Privacy Management, 61, 75.

[722] *Urban and others*, in: Data Privacy Management, 61, 71 and 73.

[723] *Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 14.

[724] *Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 10f.

[725] *Veale/Binns/Ausloos*, 8 IDPLaw 2018, 105, 118-121; *Bräutigam/Schmidt-Wudy*, 1 CR 2015, 56, 62.

cc) Perspectives for Advancement

There are, however, still significant ways in which a portal designed for the submission of access requests could support individuals in the exercise of their rights, especially with regards to the extensive and frustrating administrative hurdles. One of the first obstacles is typically the identification of the individual. As outlined in the preceding text under Part 1 Chapter 2: D. I. 3. Identification, there are valid reasons behind this since the controller has to make sure any information is in fact provided to an authorised person. If this, however, was accordingly accounted for by the PIMS, a simpler solution is at least imaginable. One option would be cooperation between the portal and controllers, where a standardised identification procedure administered by the PIMS is agreed upon. In that scenario, the individuals could prove their identity once and subsequently issue requests to multiple controllers without encountering the same hurdle each time. The same could also work if a certification for such verification procedures was issued in accordance with Article 42 and 43 and a portal obtained such. In that case, controllers could trust the checks previously conducted by the PIMS. Such an approach would not only make the procedure significantly easier for individuals, but for companies as well, which frequently struggle with assuring all necessary precautions have been taken.

Another small but yet compelling feature would be the automatic calculation of deadlines. With companies notoriously not answering requests at all, answering late, or using different principles for the determination of the time limit, it is frequently unclear for individuals by when they should have received a response.[726] In that sense, a timer counting down the time left to respond could again be useful to both individuals and businesses. Interestingly enough, many compliance management platforms (see Part 1 Chapter 1: A. III. Compliance Management) for businesses do include the option of tracking

---

[726] *Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 8; *Urban and others*, in: Data Privacy Management, 61, 71.

deadlines.[727] However for some reason, this functionality has apparently not yet infiltrated the realm of PIMS. The potential of such does not, however, only lie in informing the parties when a deadline has been exceeded. Additionally, automated reminders could be generated for the user, taking away this burdensome task from them.

Last but not least, quality control of requests should be considered. As already outlined in the context of transparency enhancing PIMS (see Part 1 Chapter 2: B. III. Proposals for Improvement), machine learning and natural language processing can, to a large extent, verify the presence of certain information as well as audit its accuracy. Users generally struggle with obtaining the relevant details, as responses to requests rarely seem to actually provide a full overview.[728] Also, data subjects report often receiving a generic standardised text, rather than an actual description of the specific processing relating to their personal data, even where explicit questions about such were submitted to the controller.[729] Participants did, however, seem to get better quality results after following up on the issue.[730] In that sense, a combination of a verification functionality with an automated follow-up would in fact present an immense improvement for individuals. After the submission of an answer by the controller, the PIMS could at first perform an automated check, reviewing if all legally required information is present and if the specific questions of the data subject have been answered (the individual

---

[727]For example: One Trust, https://www.onetrust.com/products/privacy-rights-automation/?utm_source=google&utm_medium=cpc&utm_campaign=DACH OneTrust Privacy&utm_content=DSAR SAR&utm_term=dsar tools&gclid=EAIaIQobChMI2ryXx7eC-gIVko1oCR3e-AwoEAAYAiAAEgJdwPD_BwE (accessed: 16 October 2025); HiScout, https://www.hiscout.com/checkliste-datenschutz/ (accessed: 16 October 2025); DataGuard, https://www.dataguard.com/platform (accessed 16 October 2025).

[728]*Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 11.

[729]*Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 12f; *Urban and others*, in: Data Privacy Management, 61, 73; *Zimmer*, Streamingplattformen, 46.

[730]*Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 12; *Ausloos/Dewitte*, 8 IDPL 2018, 4, 15.

could, for example, be provided with a selection within the portal before sending the request). If the tool finds any gaps or inconsistencies, an automated follow-up could be sent to the controller asking for verification.[731] In the same vein, the "auditing functionality" (see Part 1 Chapter 2: B. III. 2. Auditing) could also be transferred in order to review omissions in the controller's statement.[732] This would have the advantage of sparing the data subject the enormous workload stemming from such a chain of replies. It would also allow the controller to verify their answer without instantaneously being threatened with DPA involvement. There should also be minimal harm for businesses which provided all relevant details in the first instance, since a simple confirmation that all has been verified and seems to be in order would suffice.

dd) Existing Initiative: Access My Info

Considering the practical relevance of the right to access, the already existing technical possibilities and the potential for improvement presented earlier, it is to an extent surprising that no widely known systems or initiatives working on the development of such seem to have been formed. One tool, however, that does aim at lowering the administrative hurdles of individuals in creating access requests is Access My Info.[733] The application assists individuals with the generation of a customised access request but at the time of writing, was only able to create such for Canada and Hong Kong.[734] It

---

[731]For example: "Our analysis shows that information regarding the legal basis for processing has been left out. Please verify." or "The submitted request contained questions regarding profiling. Your answer does not seem to acknowledge that point. We would kindly ask you to verify your response and provide additional details where necessary".

[732]For example: "You informed us that no personal data of person XYZ is being processed in your systems. An automated analysis of the application's binary code however revealed the presence of multiple tracking components. We would therefore ask you to verify your answer and explain possible inconsistencies."

[733]*Hilts/Parsons*, PETS 2015, 1.

[734]Acces My Info Citizen Lab, https://accessmyinfo.org/ (accessed: 29 March 2026).

also does not send out the request automatically but rather asks the user to submit such personally.[735] This was a premeditated decision by the creators in order to assure that data subjects would actually exercise their autonomy.[736] While understandable, the offered functionality is in that sense limited in the extent that they could enable a greater public to the exercise of their rights.

c) Copy

In addition to being entitled to receive information about the details of each processing activity concerning them, data subjects also have the right to be provided with a copy of the personal data undergoing processing in accordance with Article 15(3). The extent of this right is, however, still debated.[737] Furthermore, the relationship between this right, the general right to access, and the right to data portability is *often* questioned.[738]

aa) Relationship with the Right to Information

With regards to the right to portability, while the comparison is understandable this needs to be considered as a separate right. The claim under Article 20 only covers certain very specific circumstances (the data provided to the controller, legal basis is consent or performance of contract, processing carried out by automatic means etc.) and is thereby far less extensive. The right to access, on the other hand, does not mention any specific format in which data should be provided. Most importantly, however, these two rights pursue different purposes. Whereas Art. 15 aims at assuring that individuals can obtain full disclosure as to the processing of personal

---

[735] *Hilts/Parsons*, PETS 2015, 1, 2.

[736] ibid.

[737] *Engeler/Quiel*, 31 NJW 2019, 2201, 2201; *Lembke/Fischels*, 8 NZA 2022, 513, 513; *Brink/Joos*, 11 ZD 2019, 483, 483; *Wybitul/Brams*, 10 NZA 2019, 672, 627ff.

[738] Kühling/Buchner / *Bäcker*, Art. 15, para 39; Paal/Pauly / *Paal*, Art. 15 DSGVO, para 33; *Zikesch/Sörup*, 6 ZD 2019, 239, 239f.

data concerning them, Art. 20 predominantly tries to enable competitiveness between controllers, as well as a free choice on the consumers' side.[739] Some also consider the information rights as a form of prerequisite to the other individual rights, as they intend to provide the subject with the necessary facts in order to determine their further actions, thereby creating a basis for the decision-making process.[740]

bb) Relationship to other Access Modalities

As for the different elements of the right to access (confirmation, details, copy and access only), it would be most logical to consider all of these as separate modalities of one extensive right which complete each other, yet may be invoked by the data subject based on their individual needs.[741] Whereas in some instances a simple confirmation of whether or not processing is taking place or a general overview of the type of processing might be sufficient for an individual, some might require a deeper insight. The different modalities can, however, not be considered the same, as they, to an extent, provide different information and serve a different purpose. For example, while a copy would most accurately present what kind of personal data is being processed, it will most likely not give the data subject any insight into the legal basis of processing or transfers to third parties.[742] In that sense, considering these rights as mutually exclusive would have a devastating effect on the rights and freedoms of the individual, since they would to a large extent be hindered in gaining a full understanding of the underlying processing.[743]

On the other hand, while these modalities do constitute one general right based on practical considerations, controllers should not be obliged to automatically fulfil all modalities if one part of the right is being invoked. In consideration of the principle of data minimisation,

---

[739]Kühling/Buchner / *Herbst*, Art. 20, para 4; *Brink/Joos*, 11 ZD 2019, 483, 484.

[740]*Sobolčiaková*, 12 MUJLT 2018, 221, 223.

[741]Kuner and others / *Zanfir-Fortuna*, Art. 15, 449, 464f; *EDPB*, Guidelines 01/2022, para 23; *Zikesch/Sörup*, 6 ZD 2019, 239, 240.

[742]*Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 15 DSGVO, para 28.

[743]*Brink/Joos*, 11 ZD 2019, 483, 483.

it would, for example, be completely disproportionate to provide a large file with all datasets if an individual simply requested information on the legal basis for processing. Such an overflow of information would in fact not be expedient, as it could potentially overwhelm the data subject, thereby reducing comprehensibility and transparency.[744] It might also, to an extent, go against the principles of integrity and confidentiality, as any additional processing of personal data will always have certain security implications. If, on the other hand, the individual did not mention a specific query in their submission but simply communicated the wish to exercise their right under Article 15, then the controller would in principle be required to fulfil all modalities.[745]

cc) Request Specification

Such largely unspecified requests are, however, the common reality for controllers across sectors, where even mentioning the legal basis is not a given. This practical issue in part stems from the fact that while the GDPR places a number of requirements on controllers as to the form in which answers are to be provided, there are no legal stipulations for data subjects as to the form or content for submitting data subject requests.[746] Only Recital 63 mentions the fact that where a controller processes a substantial amount of information about an individual, they should be able to request a specification from the data subject as to which processing activity the request concerns. Recitals, however, are not legally binding and the simple possibility of seeking specification also does not stipulate an obligation on the side of the data subject to actually do so.[747] Such a general simplification of matters on the side of the individual is more than justified in the context of the general imbalance of powers between

---

[744]*EDPB*, Guidelines 01/2022, para 35 b).

[745]Kuner and others / *Zanfir-Fortuna*, Art. 15, 449, 464.

[746]Kuner and others / *Zanfir-Fortuna*, Art. 15, 449, 465; *EDPB*, Guidelines 01/2022, para 50; *DSK,* Kurzpapier Nr. 6, 1.

[747]Eßer/Kramer/von Lewinski / *Stollhoff*, Art. 15, para 39; Ehmann/Selmayr, *Ehmann*, Art. 15, para 54.

data subjects and controllers and is directly in line with the requirement of facilitation. It does, however, lead to uncertainty on the side of the business, as well as incoherent actions, ultimately resulting in unsatisfactory and either too broad or too detailed answers for consumers.

This predicament could, however, most likely be salvaged by simply enquiring as to the exact purpose of a request in advance. In the current market, many controllers still do not bother to provide a specific contact channel for an access request or the exercise of any other data subject rights for that matter.[748] Those who do mention the DSRs directly in their privacy policy, in most instances simply refer to a functional email address to be contacted for all data protection related matters.[749] Even those who do offer a specific contact form for users in which relevant details could be provided, seem to opt mainly for questions assuring identifiability rather than enquiry specification.[750] All the more worrying is the substantial amount of paper-based request forms still found online, which also do not provide any guidance towards specifying such requests other than containing some sort of open question where individuals are free to enter

---

[748] *Ausloos/Dewitte*, 8 IDPL 2018, 4, 15.

[749] For example: Wikipedia, https://foundation.wikimedia.org/wiki/Privacy_policy#Contact_Us (accessed: 15 April 2026): *"If you are located in the European Economic Area and have questions about your personal data or would like to request to access, update, or delete it, you may contact our representative via email at EUrepresentative.Wikimedia@twobirds.com, or via mail [...]"*; ICO, https://ico.org.uk/global/privacy-notice/your-data-protection-rights/ (accessed: 15 April 2026): *"Please contact us at accessicoinformation@ico.org.uk if you wish to make a request, or contact our helpline on 0303 123 1113."*; Spotify, https://www.spotify.com/us/legal/privacy-policy/#11-how-to-contact-us (accessed: 15 April 2026): *"For any questions or concerns about this Policy, contact our Data Protection Officer any one of these ways: email privacy@spotify.com write to us at: Spotify USA Inc., 150 Greenwich Street, Floor 62, New York, NY 10007, USA"*.

[750] For example: Hillingdon Council, https://www.hillingdon.gov.uk/article/2479/Subject-access-request-form (accessed: 15 April 2026); CWT, https://www.mycwt.com/legal/sar-form/ (accessed: 15 April 2026); ESB, https://esb.ie/data-privacy/esb-and-your-data/general-data-protection-regulation-gdpr-request-form (accessed: 15 April 2026).

additional details.[751] Such open questions, however, most likely remain largely ineffective, as individuals who are unsure about the specific extent of their rights will simply leave these fields blank since they are not mandatory. What could, however, be considered both constructive and convenient would be fine grained drop-down options, allowing the person to specify their intent while at the same time transparently disclosing what alternatives are actually available. In that sense, the data subject could, for example, first select which rights they would like to exercise. Once one or more are selected, additional questions could appear.[752] This process could incorporate multiple questions, always offering concrete options for actions.[753] The construction of such a form can truly not be considered complicated but would in fact have immense potential for improving the process for all parties involved. Data subjects would be provided with concrete guidance and suggestions as to what can be expected, whereas controllers would receive a request with a specified objective and therefore avoid any unnecessary workload. While controllers can implement such a solution on their own, they can also not be forced to do so. In that sense, a standardised offering from a PIMS provider would most likely be the most effective option for data subjects. This could also have the advantage of facilitating significant

---

[751]University of Cambridge, https://www.information-compliance.admin.cam.ac.uk/files/cambridge_subject_access_request_form.pdf (accessed: 15 April 2026); Department of Enterprise, Trade and Employment, https://enterprise.gov.ie/en/publications/dp-subject-access-request-form.html (accessed: 15 April 2026); Opus Restructuring LLP, https://opusllp.com/wp-content/uploads/2020/10/Opus-GDPR-Data-Subject-Access-Request-Form-02-040220.pdf (accessed: 15 April 2026).

[752]For example, if the person selected “access”, they would be asked if they want a) details of their processing activities; b) a copy of their data; c) remote access to their data; or d) all of the above.

[753]For example, if “details of processing activities” were selected, the system could go further asking if details should be provided about: a) the purposes of the processing, b) the categories of personal data concerned, c) recipients, d) storage periods, e) other data subject rights, f) the source of data, e) automated decision making. Another option would be the specification of certain types of processing, such as a) advertising, b) account management, c) research etc.

improvements over time. A system handling a substantive amount of requests on an everyday basis will have more data and feedback available to optimise the details of the questionnaire over time.

dd) Format of the Copy

The described functionality could also, to a certain extent, ease the general consternation regarding the specific form in which copies are to be provided. Other than determining that in instances where requests are being made electronically, the relevant information should be provided in a "commonly used electronic form" (unless the data subject specified otherwise), the GDPR does not contain much guidance on that issue. In literature, as well as the relevant case law, questions concerning the extent of the claim, what exactly constitutes a copy, and what kind of format could or should be used are therefore subject to much debate.[754] Consequently, it comes as no surprise that practices in that area show significant discrepancies as well, with information being provided in varying degrees of detail and a multitude of formats.[755] While a general adaptability to the circumstances at hand might be justified, these disparities can additionally aggravate the already present confusion on the side of the data subjects. In that sense, the previously mentioned request specification functionality could also allow the individual to select what type of format the information should be provided in. While controllers would not necessarily be forced to oblige with the requested format,[756] the Guidelines of the EDPB do underline that they should *"keep in mind that the format must enable the information to be presented in a way*

---

[754]*Brink/Joos*, 11 ZD 2019, 483, 487; Ehmann/Selmayr, *Ehmann*, Art. 15, para 68-70; Eßer/Kramer/von Lewinski / *Stollhoff*, Art. 15, para 35; *Spindler*, 16 DB 2016, 937, 944; Kühling/Buchner / *Bäcker*, Art. 15, para 40f; *Engeler/Quiel*, 31 NJW 2019, 2201, 2202f; *Lembke/Fischels*, 8 NZA 2022, 513, 515ff; *Hartung/Degginger*, 46 DB 2021, 2744, 2744f.

[755]*Sørum/Presthus*, 34 Inf. Technol. People. 2021, 912, 924; *Urban and others*, in: Data Privacy Management, 61, 71f.

[756]Kühling/Buchner / *Bäcker*, Art. 15, para 40.

that is both intelligible and easily accessible"[757]. To this end, the preferences of the data subject should at least be taken into consideration.

ee) Security of the Copy

While the right to access lies at the heart of enabling individuals to gain control over their personal data, it can simultaneously pose a significant threat to the same cause if abused by others.[758] Studies performed in the field have unfortunately evidenced that procedures established by controllers *often* are lacking in the necessary security measures.[759] This pertains mainly to the identification of individuals and the modalities through which data is being transferred to them.[760] Such vulnerabilities leave data subjects at great risk. Personal Information Management Systems could therefore support these rights not only by ensuring secure identification but also secure transfers of information concerning them.

d) Access Only

Whereas the right to access can be facilitated by providing individuals with all relevant details pertaining to the processing of their personal data or by simply handing over a copy of all existing datasets, there is also the possibility of allowing them to directly access the data in question. Recital 63 specifically mentions that controllers should, as far as possible, enable direct remote access through secure systems. While a permanent form of access is generally preferred for the purposes of full transparency and intelligibility, non-permanent modalities, such as time-limited remote access without the option to download files, on-site inspections, or even the provision of oral information might be considered appropriate in certain cases,

---

[757] *EDPB*, Guidelines 01/2022, para 150.

[758] *Di Martino and others*, in: USENIX 2019, 371, 371.

[759] *Di Martino and others*, in: USENIX 2019, 3711, 374-379; *Bufalieri and others*, IEEE 2020, 75, 75ff.

[760] *Bufalieri and others*, IEEE 2020, 75, 79-81.

especially when other interests are to be considered.[761] Such a restriction of the right to access is also supported by Art. 15(4), which postulates that rights and freedoms of others should not be adversely affected by it, thereby adding another specific exemption. While the clause technically only refers to the right to obtain a copy, it should by analogy and where necessary apply to the details provided under Art. 15(1) GDPR as well.[762] This understanding is also supported by Sentence 5 of Recital 63 GDPR and the Guidelines of the Art. 29 WP.[763]

Recital 63 also supports the notion that the rights and freedoms which should be taken into account are not limited to those of a natural person but include those of the controllers and other businesses as well, as it specifically includes the wording *"trade secrets or intellectual property and in particular the copyright protecting the software"*. It is, however, important to note that Art. 15(4) constitutes more of a restriction rather than an exemption in that sense, since it does not allow controllers to completely deny access but solely supports consideration of the less intrusive means of access such as partial access or less granular information where necessary and appropriate.[764] In that sense, this restriction might therefore also, to a certain extent, affect the usability of Personal Information Management Systems. While the use of PIMS has the potential to add a certain layer of security to the overall processing,[765] it also adds another party to the circumstances. Based on the actual configurations within such a platform, the PIMS provider should in principle not be able to access any personal data or details regarding such. Depending on

---

[761]*EDPB*, Guidelines 01/2022, para 133.

[762]*Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 15 DSGVO, para 34; *Custers/Heijne*, 46 CLSR 2022, 105727, 7.

[763]*Art. 29 WP*, Guidelines on Automated individual decision-making, 17.

[764]Kühling/Buchner / *Bäcker*, Art. 15, para 42a; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 15 DSGVO, para 34; *Art. 29 WP*, Guidelines on Automated individual decision-making, 17; *Hacker/Passoth*, in: xxAI, 343, 350.

[765]See Part 1 Chapter 2: A. III. 2. a) Confidentiality; D. I. 3. Identification and D. II. 1. c) ee) Security of the Copy.

the type of storage,[766] the information might, however, still be processed through their systems. If the disclosed datasets affect the rights and freedoms of others, however, a processing by a third party (the PIMS) might be considered unproportionate and give the controller a basis for declining the use of this channel and insist upon forms of access only involving the data subject itself.

e) Interim Conclusions: Access

The right to access under Article 15 of the GDPR contains four independent components. These are the right to: (1) obtain a confirmation of and (2) details about the processing, as well as the right to request (3) a copy of or (4) direct access to the individual's personal data.

The right to obtain a *"confirmation as to whether or not personal data concerning him or her are being processed"*, enshrined in Art. 15(1) clearly supports the validity of precautionary requests, where no personal data about an individual is in fact being processed, or where the individual is not certain about that fact. Personal Information Management Systems supporting a type of "pre-confirmation functionality" will do so by conducting searches on the client's mailbox, the dark web, or various databases identifying where the client's personal data is being held and thereby creating an initial overview of potential controllers to be contacted, for the exercise of the right to access, or other data subject rights.

Where a controller has confirmed the processing of personal data towards a data subject or where that person is already aware of the existence of such, the individual can demand to receive detailed information regarding the processing activity in question. While these types of requests are quite popular and businesses have in general adjusted their internal procedures to the facilitation of such, studies still report dissatisfaction of customers with the provided answers, in particular in terms of empowerment and transparency. This is largely based on the receipt of delayed and generalised answers, as well as

---

[766] See Part 1 Chapter 2: A. I. Technical Architecture.

the omission of facts relevant to the individual. In that regard, Personal Information Management Systems have a great potential to alleviate these administrative hurdles. This could, for example, be achieved through undertaking an identification procedure on behalf of multiple controllers or by calculating and monitoring deadlines. Most importantly, however, the already existing technical developments in the areas of machine learning and natural language processing, presented in the context of transparency enhancing technologies, may be applied in order to incorporate a type of automated quality control, which would inform controllers about missing details on behalf of the data subject. In the same vein, the auditing functionalities described in that context could also be transferred in order to review the accuracy of statements made by the controller.

In addition to being entitled to receive information about the details of each processing activity concerning them, data subjects also have the right to be provided with a copy of the personal data undergoing processing in accordance with Article 15(3). Since this right typically raises a number of questions as to the relationship between this and the other access modalities, as well as the relation to data portability, the potential advancement of the quality of answers provided by controllers through a form of request specification via the PIMS has been considered in this context. This could, for example, be facilitated through a menu containing fine grained drop-down options, allowing the person to specify their intent while at the same time transparently disclosing what alternatives are actually available. Here, the exact format of the requested copy could also be defined.

While permanent forms of access such as the provisions of written details about the processing activity or an entire copy of the individual's personal data, are generally preferred for the purposes of full transparency and intelligibility, Art. 15(4) and Recital 63 also support the idea of introducing non-permanent access modalities such as time-limited remote access, without the option to download files, on-site inspections, or even the provision of oral information. These might especially be considered appropriate when interests of others might be affected. In the context of PIMS, this issue will be quite relevant as these types of tools, while potentially adding security to the

handling of data subject request, also add another party involved in the processing activity, which needs to be accounted for. Whereas the PIMS provider should in principle not be able to access any personal data or details regarding such, they will, depending on the type of storage deployed within the platform, still be processing the information in question. Such processing by a third party might therefore, depending on the circumstances, be considered disproportionate where the disclosed datasets affect the rights and freedoms of others, thereby giving the controller a basis for declining the use of this channel.

2. Rectification

Article 16 of the GDPR contains two modalities of rectification: the right to have inaccurate personal data corrected and to have incomplete personal data completed. This claim directly stems from the principle of accuracy enshrined in Art. 5(1)(d), in accordance with which personal data should be accurate and kept up to date. The significance of keeping information correct has been a part of European and international data protection law since its infancy.[767] It has also largely remained undisputed, since it is generally considered that the use of correct data for any sort of processing would in principle benefit both the controllers as well as the data subjects.[768] While there is some debate with regard to the relationship to data quality[769] and the applicability of the right towards opinions,[770] these questions have little practical relevance in the context of Personal Information Management Systems and should therefore not be further explored here. What is, however, relevant is the question as to what extent PIMS could assist data subjects with the execution of

---

[767] *Hallinan/Zuiderveen Borgesius*, 10 IDPL 2020, 1, 2; Kuner and others / *de Terwangne*, Art. 16, 469, 471f.

[768] On the opposite idea of using „inaccurate" personal data for data protection purposes refer to: *González Fuster*, 12 Ethics Inf Technol 2010, 87, 87ff; *Chen*, 4 EDPL 2018, 36, 36ff.

[769] *Dimitrova*, 12 EJLT 2021, 1.

[770] *Hallinan/Zuiderveen Borgesius*, 10 IDPL 2020, 1, 2ff.

this right. The two possible functionalities which should be considered in this context are (1) direct rectification and (2) multi-controller submissions.

a) Direct Rectification

The first functionality would entail the possibility for the individual in question to directly verify, amend, update, or complete their personal data. This would naturally work for systems where data is already hosted either with the PIMS or locally on the user's device. Since storage is one of the features considered and applied in PIMS,[771] it is only logical for such to incorporate the option of direct rectification as well. In that sense, this functionality will most likely never be a "stand-alone feature" but rather another way in which systems already, including secure storage, could further enable individuals to take control of their personal data.

In the same vein, the option of direct or automatic rectification could most likely be incorporated into PIMS with the underlying objective of enabling data access through consent management.[772] Here, a communication channel between controllers and PIMS will already have to be in place and should further be used accordingly. Rectification could be facilitated through the creation of a link between the different data stores, causing direct correction or changes to certain datasets across systems, once such a change has been triggered in the PIMS. Another less sophisticated but also easier to implement, alternative would be the automatic signalling of necessary updates across controllers, working similarly to an alarm system.

Such a signalling feature could also be implemented in combination with PIMS facilitating access requests.[773] Where, for example, a copy of the data or details of processed data categories are being submitted, the PIMS could include an algorithm comparing the data

---

[771]See Part 1 Chapter 2: A. Storage.
[772]See Part 1 Chapter 2: C. IV. Proposals for Improvement.
[773]See Part 1 Chapter 2: D. II. 1. Access.

contained in the reply with the individual's information stored in the system or communicated by other controllers. Any inconsistencies could be flagged to the data subject for verification accordingly and, once the accuracy of such has been confirmed or denied, the need for correction could be communicated to the relevant controllers.

While the idea of direct rectification works very well in the outlined combinations, the establishment of such as a stand-alone feature might, however, be difficult; although remote access to the controller's systems in order to trigger direct changes or facilitate data verification could be technically possible, it would also most likely be difficult to actually enforce. Controllers may in most instances be unwilling to allow third party access to their data stores, either based on security concerns or for a simple lack of incentives.

b) Multi-Controller Submissions

Where the direct rectification cannot be facilitated, Personal Information Management Systems may, however, provide the option of submitting the same request to multiple controllers. This would be particularly helpful in circumstances such as moving, changing one's bank account or cell-phone number, as this typically triggers the unfortunate need to inform a multitude of parties at once. On the one hand, individuals can keep an overview of relevant contacts within the platform. In that case, the functionality would, however, lack substantial differentiation from a standard directory. However, as outlined under Part 1 Chapter 2: D. II. 1. a) bb) Pre-Confirmation, tools performing automated searches on the individual's mailbox or other sources in order to identify potential data controllers and generate automated deletion requests for such already exist. In that sense, the same functionality could most likely also be expanded to apply for requests for rectification.

3. Erasure

Article 17 of the GDPR provides data subjects with the right to obtain erasure of their personal data from the controller under specific circumstances. This right serves the objectives of not one, but

multiple principles of data protection: purpose limitation, data minimisation, storage limitation and, in a sense, integrity and confidentiality as well.[774] Being able to not only refuse disclosure of personal information but also have it removed lies at the heart of the idea of informational self-determination, which is directly linked to the concept of human dignity.[775] This right is also not new within the European realm of data privacy. Art. 12b of the Data Protection Directive (DPD) already provided that data subjects should be able to obtain *"as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive"*.[776]

While the formal designation of "right to erasure" was already used under the Directive, the term "right to be forgotten" is much more present in the general consciousness and is also commonly used in academic literature as well.[777] Tracing back the exact historic routes of this concept would be difficult,[778] but the topic has definitely gained rapid significance over the last decades in the context of online data processing and digital memory.[779] After all, the saying "the internet

---

[774]Schwartmann/Jaspers/Thüsing/Kugelmann / *Leutheusser-Schnarrenberger,* 'Art. 17' DSGVO, para 6.

[775]*RouvroyPoullet*, in: Reinventing Data Protection?, 45, 58-61; *Lynskey*, The Foundations, 94-99; *Frosio*, 5 Colo. Tech. LJ 2016, 307, 313ff.

[776] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281 (Data Protection Directive).

[777]*Werro*, in: The Right To Be Forgotten, 1, 1ff; *O'Hara*, 19 IEEE Internet Comput. 2015, 73, 73ff; *Ausloos*, 28 CLSR 2012, 143, 143f; *Weber*, 2 JIPITEC 2011, 119, 120; *Holznagel/Hartmann*, 4 MMR 2016, 228, 230-232; *Buchholtz*, 12 ZD 2015, 570, 573-577.

[778]Right to forget was for example already mentioned in the 2002 publication: *Streich*, 24 New Political Science 2002, 525, 525ff. The German Constitutional Court however already referred to a "right to be left alone" in its ruling on Lebach I in 1973 (BVerfG, NJW 1973, 1226), which leads some to consider this as the foundation of its development (at least in Germany): *Kodde*, 3 ZD 2013, 115, 118.

[779]*Mayer-Schönberger*, Delete, 50-91; *Weber*, 2 JIPITEC 2011, 119, 120; *Zittrain*, The Future, 231-234; *Holznagel/Hartmann*, 4 MMR 2016, 228, 229;

doesn't forget" exists for a reason.[780] A milestone in that context was the CJEU Judgement related to *Google Spain*, which dealt with the responsibility of search engines for the indexing of information published by third parties.[781] While arguably not actually dealing with the question of "erasure" per se but rather restriction of processing, since the ruling primarily referred to the removal from a list of results independently from the erasure from the underlying webpage or a prohibition of indexing itself,[782] it is still considered a landmark decision for the right to be forgotten.[783] The question of the conflict between the right to inform and the right to be forgotten is also to this day subject to a heated, cross-Atlantic debate.[784] While there are many critics, the trend, however, seems to be heading towards global acceptance, with many jurisdictions enacting laws containing a similar legal basis.[785] Considering the growing relevance in the context of new technologies, as well as international recognition, this specific right will be of particular interest in Personal Information Management Systems. Therefore, the existing legal framework, its potential for improvement, and the possible challenges should be carefully explored.

Blanchette/Johnson, 18 TIS 2002, 33, 33ff; *Cheung*, 1 J. Media Law 2009, 191, 191ff; *Austin*, 22 Law and Philosophy 2003, 119, 119ff.

[780]*Sykes*, End of Privacy, 221; *Marks*, 23 ELR 2016, 41, 41ff; *Jandt/Kieselmann/Wacker*, 37 DuD 2013, 235, 235ff.

[781]Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.

[782]Kuner and others / *Kranenborg*, Art. 17, 475, 479.

[783]*Holznagel/Hartmann*, 4 MMR 2016, 228, 230-232; *Buchholtz*, 12 ZD 2015, 570,, 573-577; *Arning/Moos/Schefzig*, 30 CR 2014, 447, 447ff; *Bunn*, 31 CLSR 2015, 336, 366ff.

[784]*Werro*, in: Haftungsrecht, 285, 285ff; *Bennett*, 30 Berkeley J. Int. Law 2012, 161, 161 ff; *Arning/Moos/Schefzig*, 30 CR 2014, 447, 447ff; *De Baets*, IRLCT 2016, 57, 57ff; *Walker*, 64 Hastings L.J. 2012, 257, 257ff; *O'Hara*, 19 IEEE Internet Comput. 2015, 73, 73ff; *Ausloos*, 28 CLSR 2012, 143, 143ff.

[785]*Werro*, in: The Right To Be Forgotten, 1, 1ff.

a) Grounds for Application

Article 17(1) sets out specific grounds under which the right to erasure should apply. These can be broadly divided into two categories: instances dependent on a request of the individual and instances of automatic application.

aa) Automatic Application

Points (a) (*"the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"*); (d) (*"the personal data have been unlawfully processed"*) and (e) (*"the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject"*) essentially describe scenarios under which the obligation to delete the data in question already applies, independently from any action on the data subject's side.[786] In that sense, they do not constitute a typical "request" in the sense described under Part 1 Chapter 2: D. Request, as they do in fact to a large extent apply automatically and are not entirely based on the necessity of an inquiry by the individual. This means that where a data subject submits through a PIMS such a "request" for deletion under one of these grounds, this will technically constitute more of a reminder or notification for the controller as of the existence of certain facts and the consequential obligations.

bb) Application on Request

Points (b) and (c), on the other hand, do require direct actions from the data subject, namely the withdrawal of consent or an objection to the processing which could be conducted through a PIMS. While not explicitly stated, the same should be assumed for point (f) (*"the personal data have been collected in relation to the offer of information*

---

[786]Kühling/Buchner / *Herbst*, Art. 17, para 8-10, 14f; Paal/Pauly / *Paal*, Art. 17 DSGVO, para 20; *Gründel*, 11 ZD 2019, 493, 494; *Trentmann*, 33 CR 2017, 26, 30f.

society services referred to in Article 8(1)"), since the opposite assumption would lead to the paradoxical conclusion that all data processed based on a child's consent would need to be instantaneously deleted.[787] While some consider the grounds of Art. 17(1)(f) only to apply where the consent for such processing is withdrawn,[788] this makes little practical sense as there would be no significant distinction in comparison to Art. 17(1)(b).[789] It could, however, be read as an extension of the right to erasure, applicable under point (b) in the sense that it would also preclude the controllers from the use of any legal basis other than consent, even where such might be relevant.[790] This would effectively mean that the wishes of the child would be given preference over the interests of the controller, even where legally the processing could have continued.[791] Such a reading would reinforce the special protection of children's personal data, explicitly recognised in Recital 38.

Also based on the data subject's inquiry are the rights under Art. 17(2) of the GDPR. Here, it is specified that where the controller has made personal data public, reasonable steps should be taken by such to inform other businesses processing the information in question about the individual's enquiry. The Article, however, clearly refers to instances where *"the data subject has requested the erasure"*, suggesting that the same obligation does not necessarily arise in the cases of automatic application described above, unless requested by the person.[792] Such a requirement can encompass a number of practical difficulties for controllers in tracing back other entities, mak-

---

[787]Paal/Pauly / *Paal*, Art. 17 DSGVO, para 28.

[788]Paal/Pauly / *Paal*, Art. 17 DSGVO, para 28; Ehmann/Selmayr, *Kamann/Braun*, Art. 17, para 31.

[789]*Schantz*, 26 NJW 2016, 1841, 1845.

[790]Kühling/Buchner / *Herbst*, Art. 17, para 35; Paal/Pauly / *Paal*, Art. 17 DSGVO, para 28.

[791]*Gola/Schulz*, 10 ZD 2013, 475, 480; Paal/Pauly / *Paal*, Art. 17 DSGVO, para 28a); DSK, Kurzpapier Nr. 11, 1.

[792]*Hornung/Hofmann*, 68 JZ 2013, 163, 167; Kühling/Buchner / *Herbst*, Art. 17, para 52; Paal/Pauly / *Paal*, Art. 17 DSGVO, para 34.

ing use of the data in question. In that sense, the available technology and the cost of implementation should be taken account of, while determining what type of steps would still be considered as "reasonable".[793]

b) Exemptions

As with any right, the right to erasure is not boundless and there are certain circumstances under which the cessation of a certain processing activity might not be warranted. These are outlined under Art. 17(3) GDPR and apply independently from the specific ground the erasure is based on.[794] This may be quite relevant in the context of PIMS, as erasure requests submitted on behalf of the data subjects do not necessarily need to be automatically complied with. Rather the controller is given a number of circumstances under which data could still be retained against the wishes of the individual. The question therefore occurs for which exemptions and to what extent an involvement of a PIMS might be possible or even necessary.

aa) Applicability and Practical Hurdles

The two exemptions which are the most straightforward and subject to little debate are those found in points (b) and (c) of Art. 17(3) GDPR. Under Art. 17(3)(b) the data subject's personal data does not require deletion in instances where the controller is subject to a legal obligation under European Union or Members' state law which involves the processing of such data. The same applies where such processing is necessary for carrying out tasks in the public interest or exercising official authority, which have been assigned to the controller. Similarly, in accordance with Art. 17(3)(c) erasure may also be excluded where the data in question is still necessary for *"reasons*

---

[793]For details on the technical possibilities of execution please refer to: Part 1 Chapter 2: D. II. 3. c) Technical Execution, Challenges and Potentials for Advancements.

[794]Kuner and others / *Kranenborg*, Art. 17, 475, 482; Kühling/Buchner / *Herbst*, Art. 17, para 70.

of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3)". Both of these legal bases refer to the processing of special categories of personal data. Point (h) of Article 9(2) specifically covers the purposes of *"preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services"* whereas point (i) applies for processing in the area of public health, for reasons of public interest.

The other exemptions, however, might require the weighing of interests and consideration of the specifics of the case in some instances. Art. 17(3)(e) aims at preventing the deletion of data, which might be relevant in the context of a legal claim.[795] There is some debate whether the claim needs to concern an ongoing proceeding or if the potential of future litigation would also suffice.[796] The prevailing opinion in that context seems to be, that while it is not necessary for an actual legal procedure to be in progress at the exact moment of the erasure request, the controller should at least be able to convincingly demonstrate the possibility that one might occur in the near future.[797] In that context, the probability of such and its potential impact should be weighed against the interest of the data subject.[798] Such a weighing should also take into account the potential interests of third parties, where necessary. While some sources seem to limit the applicability of the exemption to legal claims of the controller,[799] such a position should not be followed. It is, after all, possible that

---

[795] *Voigt/von dem Bussche*, GDPR, 160.

[796] Wolff/Brink/v. Ungern-Sternberg / *Worms*, Art. 17 DSGVO, para 87; Ehmann/Selmayr, *Kamann/Braun*, Art. 17, para 67; *Kühling/Klar*, 10 ZD 2014, 506, 508ff.

[797] Gola/Heckmann / *Nolte/Werkmeister*, Art. 17 DSGVO, para 48f; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 17 DSGVO, para 38.

[798] Ehmann/Selmayr, *Kamann/Braun*, Art. 17, para 67; *Kühling/Klar*, 10 ZD 2014, 506, 508ff; Kühling/Buchner / *Herbst*, Art. 17, para 83; Wolff/Brink/v. Ungern-Sternberg / *Worms*, Art. 17 DSGVO, para 87.

[799] *Voigt/von dem Bussche*, GDPR, 160.

the controller would be in possession of data which might be necessary for the establishment of a legal claim of a third party. Where the controllers are aware of these circumstances, the exemption should therefore also apply, as this would otherwise enable data subjects to effectively hinder litigation.[800]

Creating even more of a need to analyse conflicting interests is Article 17(3)(d) GDPR. It sets out a special exemption for processing operations performed for the purpose of archiving in the public interest, scientific or historical research, as well as statistical purposes in accordance with Article 89(1). Datasets necessary for the achievement of these purposes should not be subject to deletion, should this *"render impossible or seriously impair the achievement of the objectives of that processing".* This demonstrates the significance and, to a certain extent, privileged status given to those purposes by the Regulation.[801] At the same time, however, the reference to 89(1) adds the requirement of assuring appropriate safeguards for the rights and freedoms of the data subject.[802] Specifically mentioned are the principle of data minimisation and the use of pseudonymisation. The limited amount of examples has, however, been largely criticised and additional measures need to be considered as far as possible.[803] It should also be noted that it is not sufficient for the erasure to simply impede or interfere with the achievement of these objectives, but rather that they would need to be rendered impossible, meaning that it should not be interpreted too widely and consider the specific purpose at hand, especially where the individual personally requests the destruction.[804]

---

[800]Wolff/Brink/v. Ungern-Sternberg / *Worms*, Art. 17 DSGVO, para 87.

[801]*Chico*, 128 Br. Med. Bull. 2018, 109, 110; *Becker and others*, 30 EJHL 2023, 129, 145-151; *Rossnagel*, 4 ZD 2019, 157, 159; *Weichert*, 1 ZD 2020, 18, 18ff; *Johannes/Richter*, 41 DuD 2017, 300, 300ff.

[802]Kühling/Buchner / *Herbst*, Art. 17, para 82; Sydow/Marsch / *Peuker*, Art. 17, para 67.

[803]Kuner and others / *Svanberg*, Art. 89, 1240, 1247.

[804]Kühling/Buchner / *Herbst*, Art. 17, para 82; Kuner and others / *Svanberg*, Art. 89, 1240, 1246 (in relation to the narrow interpretation for the scope of the derogations put forward by Member States.

Each of the privileged purposes under Article 17(3)(d) comes with its own specific set of considerations which need to be accounted for, while weighing the varying interests of the general public, the controller, third parties, and the data subject.[805] The importance the lawmakers place on finding striking a balance between those varying objectives is also underlined, although the mention in no less than eight Recitals (156–163) evidences the extensive amount of deliberations that went into the subject matter. Further complicating this already confounding environment is the fact that Member States are also given the authority to provide specific derogations for the other data subject rights.[806] Since research projects are, however, *often* subject to international co-operations, all Member States rules would need to be considered accordingly. Controllers processing personal data for the purposes of statistics, archiving in the public interest, and scientific or historical research receiving an erasure request are therefore left with the task of assessing the importance of the overall objective for themselves, third parties, and society in general against the interests of the specific individual, while also considering all risks related to these largely complex processing activities, as well as existing national legal derogations, rules and guidelines.

Last but not least, the exemption under point (a) of Art. 17(3) needs to be considered. In accordance with this Article, the right to obtain erasure from the controller does not apply where the relevant information is necessary for the exercise of the rights of freedom of expression and information. The conflict of these two objectives is in no way new and has been discussed at length long before the GDPR came into force.[807] It was the pivotal point in the case of

---

[805] See for example: *Molnár-Gábor*, 137 Hum. Genet. 2018, 619, 619ff; *Staunton*, in: GDPR and Biobanking, 91, 91ff; *Wirth*, 8 ZUM 2020, 585, 587f; *Peloquin/DiMaio/Bierer/Barnes*, 28 Eur. J. Hum. Genet. 2020, 697, 697ff; *Weichert*, 1 ZD 2020, 18, 22f.

[806] For an overview of the currently applicable national legislation, guidelines and codes of conduct refer to: *Kindt and others,* 'Legal study on the appropriate safeguards.

[807] See for example: *Ticher*, Data Protection Vs Freedom of Information; *Charlesworth*, 15 Inf. Commun. Soc. 2011, 85, 85ff; *Meredith*, 330 BMJ 2005, 490,

Węgrzynowski and Smolczewski v Poland, brought before the European Court of Human Rights (ECHR) in 2007.[808] Here the applicants were trying to obtain an order for the removal of an article placed in the newspaper Rzeczpospolita, which alleged that their fortune was a result of assisting politicians in shady business dealings.[809] While a libel case against the newspaper was won, national courts considered ordering the complete removal of the article to constitute censorship and the rewriting of history.[810] In its Judgement on July 16, 2013, the ECHR essentially agreed with the prior assessments of the domestic courts, underlining the importance of internet archives as constituting an essential source for education and historical research.[811] In consideration of that fact, it was decided that appropriate balance between Articles 8 and 10 of the Convention had been struck.[812]

More extensive consideration on the weighing of the right to data privacy against freedom of expression were unfortunately missing from the ECJ's Judgement in the case of *Google Spain*, which has been subject to criticism from multiple sources.[813] The point of contention is also clearly evidenced in the Opinion of the Advocate General Niilo Jääskinen,[814] who not only considered the rights of the

---

490f; *Turle*, 23 CLSR 2007, 167, 167ff; *Buchner*, Selbstbestimmung, 80-102; *Roßnagel*, 1 MMR 2007, 16, 16ff; *Gola*, 48 NJW 1993, 3109, 3110ff; *Gallwas*, 44 NJW 1992, 2785, 2785ff; BVerfG, BVerfGE 78, 77; BVerfG, BVerfGE 27, 71.

[808] *Węgrzynowski and Smolczewski v Poland* App no. 33846/07 (ECtHR, 16 July 2013).

[809] ibid para 6-9.

[810] ibid para 12.

[811] ibid para 59.

[812] ibid para 68.

[813] *Kranenborg*, 1 EDPL 2015, 70, 77; *Frantziou*, 14 Hum. Rights Law 2014, 761, 767-772; *Kulk/Zuiderveen Borgesius*, 2 EDPL 2015, 113, 113ff.

[814] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, Opinion of AG Jääskinen.

search engine provider and the data subject but those of web-publishers[815] and other internet users[816] as well. The Advocate General also explicitly warned the court against concluding that the right of privacy and freedom of information could be balanced by search engine providers on a case-by-case basis, as this might potentially lead to the standardisation of an automatic take-down practice, as a result of the large volume of requests, as well as fear of liability for a lack of action.[817] These concerns might arguably have come true, with Google reporting the receipt of 1.319.407 in their Transparency Report as of 14.09.22.[818]

Regardless of the particular stance taken towards the ruling in *Google Spain*, the surrounding controversy, as well as continuing debate on the weighing of these two rights, clearly evidence the difficulties controllers might encounter in the context of handling erasure requests. While large international conglomerates with entire teams of lawyers might at least theoretically be equipped to conduct a case-by-case analysis, accurately reflecting the extent given to certain rights by both national and international law, jurisprudence and courts, this is most certainly not the case for regular small and medium sized businesses. It can, however, not be excluded that such might still be required to deal with very significant enquiries. Most importantly, adding to that predicament is the fact that the outcome of such an analysis will not only impact the rights and freedoms of the data subject and the controller but those of a potentially unlimited number of individuals looking to access certain information. Leaving

---

[815]ibid para 134: "*This would entail an interference with the freedom of expression of the publisher of the web page, who would not enjoy adequate legal protection in such a situation, any unregulated 'notice and take down procedure' being a private matter between the data subject and the search engine service provider*".

[816]ibid para 131: "*An internet user's right to information would be compromised if his search for information concerning an individual did not generate search results providing a truthful reflection of the relevant web pages but a 'bowdlerised' (94) version thereof*".

[817]ibid para 133.

[818]Google Transparency Report, https://transparencyreport.google.com/eu-privacy/overview?hl=pl (accessed: 22 October 2025).

such a crucial decision to one of the directly involved parties seems not only risky but potentially dangerous, especially if complete, irreversible deletion of information is achieved as a result. Such an outcome can in no means be considered as acceptable for the protection of the rights and freedoms of individuals, which is why measures of remediation should be considered.

bb) Reflections on Potential Advancements through PIMS

As evidenced above, controllers might encounter multiple difficulties in assessing the applicability of the exemptions found under Article 17(3) of the GDPR. The risks for the occurrence of an accidental misinterpretation are relatively low in instances of 17(3)(b) (*compliance with a legal obligation*) and (c) (*reasons of public interest in the area of public health*), as those require the existence of an explicit legal basis in European Union or Member State law, leaving the consideration of the various interests at stake largely to the lawmaker. The same can, however, not be said about the other grounds for refusing erasure of personal data. Point (e) (*establishment, exercise or defence of a legal claims*) already calls for the potential consideration of third-party interests which controllers might not be aware of when receiving an erasure request. The most complex and burdensome assessments, however, are likely to occur under points (a) (*exercising the right of freedom of expression and information*) and (d) (*archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*). Where data subjects request the deletion of their personal data for which one of these exemptions could apply, controllers are notoriously left with the obligation to weigh all potential interests against each other, in order to find an appropriate balance. This solution, however, is not only highly unsatisfactory for the parties involved, but also potentially dangerous.

First and foremost, since the controller is one of the parties whose interests are affected by the processing operation, it is at least questionable as to what extent an evaluation by such could truly be impartial. On the one hand, this concerns cases where a business might be more motivated to argue the applicability of an exemption due to their own inherent interest in continuing the processing in

question. On the other hand, however, scenarios where the controller might feel pressured to delete data for the fear of facing liability while other parties could have had an interest in the relevant information are also imaginable. This risk should not be underestimated when it comes to preserving data which might be of historical relevance, interest to research, or pivotal for the exercise of freedom of expression and/or information by another individual. Here the erroneous, pre-emptive deletion of such could have potentially disastrous consequences. Therefore, while the general premise of keeping the controllers responsible and accountable for the entire data lifecycle is absolutely justified, it might require a slight correction where the interests of other individuals are involved. In that context, the potential involvement of the Personal Information Management System could be considered.

The engagement of a third party with no underlying personal interests with regards to the outcome of an assessment could prove quite advantageous. There are, however, also a number of difficulties, which could occur as a result of the inclusion of such a functionality. First, it might be argued that such an impartial third party, which would be consulted in the decision-making process in the case of doubts, already exists, namely in the form of Data Protection Authorities. After all, Article 57 contains a large list of tasks delegated to the DPAs. Additionally, to the standard functions of enforcing the GDPR, handling complaints, and conducting investigations, there are also a number of assignments related to the support of controllers as well. The only direct reference to an obligation to provide advice to the business is contained in Art. 57(1)(l) and refers to the prior consultation in the context of the performance of a Data Protection Impact Assessment. Art. 57(1)(d), however, also obliges the Authorities to *"promote the awareness of controllers and processors of their obligations under this Regulation"*. This task is mostly being executed through the publication of guidelines, handouts, templates, toolkits

and other resources.[819] To what extent it also obliges DPAs to provide controllers with individual advice is highly debated. While some argue that it is a necessary component of the raising of awareness,[820] others deny the existence of such an obligation.[821] Although it is true that the GDPR does not mention a specific requirement to "advise" in general, limiting the scope of Art. 57(1)(d) in a way which excludes direct interactions with the processors and controllers would not be in the interest of achieving the highest level of protection for the data subjects.[822] From this perspective, it would most likely be considered highly unreasonable for a Data Protection Authority to refuse answering a direct question from a controller that concerns compliance with the GDPR. It should therefore be considered possible for businesses to contact the DPAs in instances where there is reasonable doubt regarding the applicability of an exemption under Art. 17(3) and the connected requirement to comply with an erasure request. Such a prospect of obtaining individualised advice where needed can, however, not be equated to the standardised handling of such assessments. A DPA might provide the necessary guidance and support but the actual execution of the evaluation will still be in the hands of the controller. From a practical standpoint, authorities would most likely expect controllers to be able to conduct

---

[819]See for example: CNIL, https://www.cnil.fr/fr/decisions/lignes-directrices-recommandations-CNIL (accessed: 25 April 2026); ICO, https://ico.org.uk/for-organisations/ (accessed: 25 April 2026); UODO, https://uodo.gov.pl/pl/p/poradniki (accessed: 25 April 2026); Berliner *Beauftragte* für Datenschutz und Informationsfreiheit, https://www.datenschutz-berlin.de/infothek (accessed: 25 April 2026).

[820]*Roßnagel*, Zusätzlicher Arbeitsaufwand; Kühling/Buchner / *Boehm*, Art. 57 DSGVO, para 17.

[821]*Brink*, 2 ZD 2020, 59, 59ff; Paal/Pauly / *Körffer*, Art. 57 DSGVO, para 5; Gola/Heckmann / *Nguyen*, Art. 57 DSGVO, para 15.

[822]Kuner and others / *Hijmans*, Art. 57, 927, 935 for example points out that direct engagement is also known is by some considered the most effective way of achieving compliance, which would mean that emphasis should be put on engagement and mutual understanding rather than on sanctions.

the necessary analysis on their own, once guidance has been provided. This approach would also be justified in consideration of the limited resources available to DPAs. Furthermore, controllers might be reluctant to contact the authorities too frequently, since such a practice could leave the impression that the business in question is not able to fulfil its obligations under the GDPR, possibly prompting an investigation. In consideration of these points, Data Protection Authorities cannot take on the role of an impartial third party, supporting controllers in assessing and balancing the interests connected to a data subject request.

Whereas the engagement of a third-party intermediary is most certainly a promising solution, there are some doubts whether this role could in fact be assigned to a Personal Information Management System. As outlined above, PIMS are defined as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*. It might therefore be questioned whether the provider of a PIMS can truly be considered an impartial third party. The idea behind the introduction of PIMS is after all the correction of the imbalance, which occurs between the controller and the data subject, under the current market realities. As such, the system should serve the interest of the individual, rather than both parties. However, as evidenced above, in the case of the right to erasure in particular, the rights and freedoms of other data subjects can largely be affected by the wrongful deletion of certain datasets as well. If therefore the weighing of interests was left to the PIMS provider rather than the controller, this would mostly serve the protection of the interests of those individuals. In that sense, the definition of PIMS would not necessarily have to be amended but rather its interpretation expanded to include the empowerment of individuals in the exercise of their rights in general. While the extension towards other data subjects might be feasible, the interpretation would also need to incorporate the exercise of rights other than data protection. Since the substance of the exemptions lies in the conflict between data privacy and other fundamental rights, the PIMS would consequently be tasked with the protection of those as well. Such an

expansion of the scope of Personal Information Management Systems would, however, virtually lead to the elimination of their distinctive attributes and should therefore not be supported. Thus, while the engagement of a qualified third party into the process of managing assessment, which requires the balancing of multiple interests including those of the data subject and the controller, might be a promising idea, such a functionality could most likely not be included in a Personal Information Management System sensu stricto.

c) Technical Execution, Challenges and Potential Advancements

Once the existence of grounds for erasure and the lack of applicability of an exemption have been established, the controller is required to delete the information in question without undue delay. Such a deletion should be complete, in the sense that all copies should be removed, as well as effective, meaning that no one should be able to perceive the information without the use of disproportionate effort.[823] Commonly used technical means of deletion include the overwriting of magnetic data carriers (magnetic tapes, hard or removable discs) or electronic storage devices (USB-Sticks, Solid State Drives), degaussing and incineration, as well as mechanical destruction though shredding, crushing or disintegration.[824] Anonymisation can also effectively be considered a form of erasure, since it removes the relation of data to any identified or identifiable individual.[825] In accordance with the principle of storage limitation, procedures for the timely deletion of personal data processed by the controller should already be established as part of the data protection policies within

---

[823]Kühling/Buchner / *Herbst*, Art. 17, para 37; Ehmann/Selmayr, *Kamann/Braun*, Art. 17, para 36f; *Roßnagel*, 4 ZD 2021, 188, 189.

[824]*Data Protection Authority,* Recommendation on data sanitization, 18-46; *Leeb/Lorenz*, 12 ZD 2018, 573, 573ff.

[825]*Stürmer*, 12 ZD 2020, 626, 626ff.

any undertaking.[826] While such policies mostly cover standard processes within a business, controllers still often struggle with proper implementation.[827] Any sort of initial procedural deficiencies will be even further aggravated where deletion is required based on a request outside of the standard data lifecycle management, as it requires not only the removal but also the prior localisation of all relevant datasets, with potentially different standardised deletion periods. Questions regarding the feasibility of the technical execution of an erasure request are mostly raised in the context of back-ups and the requirement to inform other parties regarding such requests, as well as the problem of deletion on the internet in general.

aa) Back-Ups

The term "back-up" refers to *"the process of making copies of data or data files to use in the event the original data or data files are lost or destroyed"*.[828] In that sense, back-ups actually constitute a central security feature used for the assurance of data integrity and availability (see Part 1 Chapter 2: A. III. 2. b) Integrity and c) Availability). Standardised short-term back-ups, which are used for the insurance

---

[826] *Hammer*, B. IV. 4. in: *Jandt/Steidle* (eds.), Datenschutz im Internet, para 211-215; Conrad/Auer-Reinsdorff / *Conrad*, § 34, para 615-630; *Roßnagel*, 4 ZD 2021, 188, 189.

[827] One of the most prominent examples of the improper implementation of erasure policies has been identified in the case of Deutsche Wohnen, whose storage and archiving system did not provide the possibility of removing data that was no longer required. The company was fined €14.5 Million by the Berlin Commissioner for Data Protection and Freedom of Information (see: https://www.edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en, accessed: 22 October 2025). While the state court terminated the process, considering the fine to be invalid based on the fact that no proof of negligence on the side of the management or legal representatives could be provided (see: LG Berlin, openJur 2021, 12957), the prosecution subsequently lodged a complaint with the Court of Appeal in Berlin (see: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210303-PM-Deutsche_Wohnen.pdf, accessed: 22 October 2025).

[828] *Rouse*, https://www.techopedia.com/definition/1056/backup (accessed: 22 October 2025).

of quick recovery in the instance of accidental loss or destruction, usually only have a storage period of a few days and are then subsequently overwritten. These should not be considered problematic in this context, as once the information has been deleted from the original system, it should also disappear automatically from the back-up within a short timeframe. Long-term back-up solutions, aiming at the archiving of an organisation's history of records, however, pose a considerable practical obstacle. One suggested solution for this issue advises on separate storage of the table containing forgotten user IDs in order to "re-forget" such, each time the back-up is restored.[829] Another proposition considers the use of cryptographic erasures, by which datasets of specific users would be encrypted upfront through the use of different encryption keys.[830] If implemented correctly, this would mean that the deletion of a single key would result in the anonymisation of such data across all systems. Whereas these approaches definitely constitute a viable enhancement of current practices, they still fail to address two significant obstacles. First of all, none of these solutions provides an option for partial deletion.[831] This might become relevant where an individual only wishes to remove certain information from their overall dataset, while still keeping other details. The same would be the case where an exemption applies to part of the information in question (for example, where a legal obligation to store data for a certain period exists), but not to all, making it necessary to remove certain parts from the overall dataset. Secondly, the suggestions of separate user ID storage and cryptographic erasures also overlook the question of the identification and deletion of unstructured data.[832]

While a Personal Information Management System will most likely not be able to solve inherent problems present in the data deletion

---

[829] *Bozhanov*, https://techblog.bozho.net/gdpr-practical-guide-developers/ (accessed: 22 October 2025).

[830] *Scope and others*, in: Database and Expert, 245, 245ff; *Sarkar and others*, in: iThings, 1-8; *Boneh/Lipton*, SSYM'96, 91-96.

[831] *Politou/Michota/AlepisPocs/Patsakis*, 34 CLSR 2018, 1247, 1251.

[832] ibid.

policy and practices of a controller, it might still be able to aid the data subject in some regards. While the outlined problems concerning data deletion are well established and obvious to any IT professional, this is not necessarily the case for each individual wishing to have their data erased. Most currently available services offering the management of deletion requests simply administer their submission and subsequently require the controller to confirm erasure of the relevant data.[833] They do not, however, request any specific proof of such. Unless, therefore, the controller in question submits a detailed explanation of their deletion procedures (which is highly unlikely), there is very little transparency as to the extent to which databases, servers and back-ups were actually inspected. Especially in instances where a data subject might have been involved with a controller through multiple channels or services, there is significant potential for only partial deletion. For example, a person might have signed up for a provider's newsletter but also applied for a job with the same company at some point in time. If the request does not specify such, an undertaking might find the person's e-mail address in the newsletter directory and assume that this was the subject matter of the request. Once the contact details are deleted, the controller might consider the request as "completed" and send a generic confirmation though the PIMS, without ever investigating the other databases. Similarly, controllers might at times neglect to fully erase data by only removing direct identifiers from the active systems but ignoring back-ups, archives and metadata related to a person. Both of these scenarios obviously constitute a serious compliance failure on the side of the controller, as businesses are required to have appropriate procedures in place which would facilitate the discovery of all relevant datasets. Since, the result could have a substantial impact

---

[833]For example: Mine, http://saymine.com/ (accessed 22 February 2026); Privacy Bee, http://privacybee.com/ (accessed 22 February 2026); DeleteMe, http://joindeleteme.com/ (accessed 22 February 2026); Revoke, http://revoke.com/ (accessed 22 February 2026); My Data Done Right, https://www.mydatadoneright.eu/faq (accessed 22 February 2026).

on the rights and freedoms of the data subject, it should be mitigated as far as possible.

One option to potentially alleviate these issues would be connected to the previously mentioned functionality of "Request Specification" (see Part 1 Chapter 2: D. II. 1. c) cc)). Since controllers are *often* overwhelmed by very general requests to "delete all data" not knowing where to start searching for such, it might be helpful for the PIMS to provide some guidance. This would be possible where this information is already present in the PIMS, either because the data was submitted through, because access requests have been previously managed by it or because the PIMS performed a prior analysis on the data subject's systems. Alternatively, where none of these apply, the data subject could be asked to fill in the necessary details, where applicable, in advance. Another option which relates less to the handling of a specific request but more to the general erasure practices of a business, would be the submission of a "checklist" in which controllers record their procedures. Such an inquiry could include reminders on typical shortcomings (Have you removed data from all back-ups? Have all copies been erased? Have all processors been informed of the request? Has the metadata related to the account been fully anonymised? etc.) and would thereby support the entity in handling the request in an appropriate manner.[834] Where certain steps cannot be performed due to technical or organisational restraints, the controller would document this fact, including a reasoning accordingly, while at the same time providing the data subject with a transparent overview of what has been done to their data.

---

[834]A similar approach has been taken by the NGO noyb when submitting complaints regarding cookie banners, which were considered not GDPR compliant. The companies received an information draft of the intended complaint, in advance to its filing and were provided with a step-by-step guide on how to change their settings, in order to comply with the law. The NGO gave each business a period of one month to adjust their banners, before filing official complaints to the Data Protection Authority. For more details see: 'noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints': https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints, 31 May 2021 (accessed: 14 October 2025).

While these functionalities could be perceived as primarily aiding the data controllers in properly fulfilling their legal obligations, they are all aimed at achieving the highest quality of data protection for the data subject and should therefore be considered as a legitimate possibility for PIMS regardless of their side effects.

bb) Internet

Another obstacle concerns the possibility (or rather impossibility) of deleting data on the internet. Due to the open nature of the web, data once published therein can easily be duplicated and reproduced. As a result, information which might initially only have resided on one server is quickly spread across various locations, which are controlled by different entities.[835] This leads to the occurrence of two main problems when it comes to the effective removal of information from the web: location of data copies and the deletion of such.[836] The removal of data from a system over which the individual has no administrative control constitutes a commonly known challenge referred to as the "hostile host problem".[837] Also, further aggravating the problem of data localisation is the existence of services such as the "way back machine", which are created explicitly for the purposes of saving and archiving information available on the web.[838] In consideration of the powerful impact the internet has on the everyday lives on individuals and consequently on their rights and freedoms, and taking into account the fact that the significance of these consequences will most likely not diminish but rather increase over the next centuries, steps need to be taken in order to assure the protection of

---

[835]*Jandt/Kieselmann/Wacker*, 37 DuD 2013, 235, 236; *Zarras and others*, in: Proceedings of the Sixth ACM Conference, 14, 14.

[835]*Kieselmann/Wacker*, 42 DuD 2018, 437, 438.

[836]*Kieselmann/Wacker*, 42 DuD 2018, 437, 438.

[837]*Kieselmann*, Data Revocation, 3; *Kieselmann/Kopal/Wacker*, 39 DuD 2015, 31, 32.

[838]Internet Archive, http://archive.org/ (accessed: 22 October 2025).

personal data. The first concepts which attempt to mitigate these issues to some extent are services relating to the expiration and revocation of information.

(1) Expiration

One idea refers to the possibility of attaching an expiration date to data published on the web. An example of a system which provides such a functionality is X-pire![839] and its successor X-pire 2.0[840]. The tool allows users to set an expiration date for images which they wish to publish on social networks or static websites. Once the previously established date passes, the image becomes automatically unavailable. One of the main problems identified in the first version related to the possibility of copying content as well as the use of decryption keys prior to the passing of the expiration date.[841] This security gap has been solved in X-pire 2.0 through the addition of measures which makes it impossible to transmit or process data in clear text by untrusted entities after publishing.[842] The system is based on ARM's trusted computing framework TrustZone, which ensures that content cannot be accessed and copied prior to the expiration date.[843] While this addition constitutes a significant improvement to the previous version, the set expiration date can still be discounted through such simple means as taking a screenshot.[844] Also, the creators admit that the system is mostly intended for an audience acting in good faith, since the used techniques can be actively deployed.[845] In that sense, website providers unwilling to cooperate with the system would be able to actively prevent the expiration of images.[846] The system's reach in terms of practical application was as of the time of writing

---

[839] *Backes and others*, arXiv preprint arXiv:1112.2649.
[840] *Backes and others*, SAC '14, 1633, 1633ff.
[841] *Gerling*, Plugging, 73; *Federrath and others*, 35 DuD 2011, 403, 406.
[842] *Gerling*, Plugging, 75.
[843] ibid 76-78.
[844] *Jandt/Kieselmann/Wacker*, 37 DuD 2013, 235, 240.
[845] *Gerling*, Plugging, 91.
[846] ibid 91.

substantially limited, since it could only be used for the expiration of images and required the use of Firefox.[847]

A multitude of other similar concepts, projects, and prototypes attempting to facilitate the automatic destruction of data over time exists on the market. Vanish, for example, is a system which endeavours to do so though integrating cryptographic techniques with global-scale, P2P, distributed hash tables.[848] Based on this method, two prototypes have been created: Fire Vanish, a Firefox plug-in for Gmail that provides the option of sending and reading self-destructing emails, and Vanishing Files, which allows users to wrap files into self-destructing vanishing data objects subject to expiration.[849] Similarly, FADE works with **F**ile **A**ssured **DE**letion for outsourced cloud storage through the use of cryptographic techniques.[850] Other projects supporting the ephemerality of data include EphPub,[851] the Ephemerizer,[852] or the Timed-Ephemerizer.[853] Whereas these are all at varying stages of development and each comes with some sort of technical constraint or gap, the underlying approach is extremely promising. Also, while they cannot be considered Personal Information Management Systems, applications such as SnapChat[854] and Proton Mail[855] do in fact constitute examples for the commercially successful implementation of the same underlying vision. The idea of self-destructing data can also be facilitated outside of the internet, for example, where the controller is given initial access to data directly though the PIMS platform. In that case, a prior setting of an

---

[847] *Federrath and others*, 35 DuD 2011, 403, 405f.

[848] *Geambasu and others*, USENIX 2009, 299, 299ff.

[849] *Geambasu and others*, USENIX 2009, 299, 307f.

[850] *Tang and others*, in: Sec. and Priv. in Comm. Net., 380, 380ff.

[851] *Castelluccia and others*, 19th IEEE, 165, 165ff.

[852] *Perlman*, 1 JISSec 2005, 51, 51ff.

[853] *Tang*, in: Public Key, 195, 195ff; *Tang*, 58 Comput. J. 2015, 1003, 1003ff.

[854] Snap Chat Privacy Policy, https://values.snap.com/privacy/privacy-policy?lang=en-US (accessed: 24 October 2025).

[855] Additionally, to features such as encryption and enhanced tracking protection the services also provided the option for self-destructing messages. See: Proton Mail, https://proton.me/mail/security (accessed: 24 October 2025).

automatic expiration date could also be used to assure timely deletion of the user's personal data.

(2) Revocation

Whereas the idea of automatic pre-determined expiration dates for data on the internet definitely constitutes a powerful step towards the regaining of privacy rights of individuals, there are, additionally to the above-mentioned technical restrictions, also a few other factors that may hinder its practicability for users. Most importantly, it requires the data subject to consider questions of privacy prior to sharing the data, making ad hoc deletion more difficult in cases where either the circumstances or position of the particular person towards the dataset or its recipient changes. As a result, alternative approaches working on the facilitation of effective and privacy friendly data deletion consider the possibility of data revocation. An example of an endeavour striving to provide the option of flexible expiration times while using a decentralised infrastructure is the Neuralyzer.[856] The system is based on a caching mechanism of public Domain Name System resolvers and has the ability to refresh information over time, while facilitating the expiration of its lifetime based on access novel heuristics.[857] Similarly to the previously mentioned methodology of cryptographic erasures, the system also works by encrypting the publicly accessible data and destroying the encryption key, once the elimination of the data is desired.[858] It does, however, also introduce a largely metric-driven revocation mechanism, which may be adapted based on various aspects such as a drop of interest or excessive access, rather than only allowing manual revocation.[859]

Another concept of an automated Data Revocation Service suggest the utilisation of unique data identifiers in order to solve the issue of locating datasets spread throughout the entire web in the first

---

[856] *Zarras and others*, in: Proceedings of the Sixth ACM Conference, 14, 14ff.
[857] ibid 23
[858] ibid 22.
[859] ibid 15.

place.[860] In addition to the assignment of such an identifier, the creation of a distributed database is suggested in order to enable data subjects (owners) to notify controllers and processors of the current status of the data.[861] This could either be facilitated through push or pull notices, meaning that the provider would either receive an automated notification regarding the demand for data to be deleted or would need to enquire about the status of a certain dataset on a regular basis.[862] The underlying idea of assigning a certain value to a dataset could in fact also be expedited further and used for the designation of other characteristics, such as "required update", "can be shared", or "subject to revision", further facilitating the other data subject rights.

cc) Multi-Controller Submissions

The described Data Revocation Service through unique data identifiers, in combination with push and/or pull notices to all relevant parties, also provides another important advantage: namely the possibility of instantaneous submission of data subject requests to all controllers at once. As already outlined under Part 1 Chapter 2: D. II. 2. b) Multi-Controller Submissions, the need to separately contact all parties potentially processing one's personal data can be burdensome for individuals. This simple inconvenience, however, amounts to sheer impossibility where data subjects can no longer foresee where their information might be located, due to the further distribution of such by their direct service providers.

The lawmakers have foreseen the occurrence of such an obstacle and have therefore introduced two types of obligation for controllers to inform other entities. First of all, where controllers have further disclosed personal data to other recipients, they are required to communicate the need for rectification or erasure of such data to those in accordance with Article 19 GDPR. This obligation can only be re-

---

[860] *Kieselmann/Wacker*, 42 DuD 2018, 437, 438.
[861] *Kieselmann*, Data Revocation, 14.
[862] ibid 15-17.

fused where it would turn out to be impossible or involve disproportionate effort. While the regulation does not provide any specific examples where such an exemption might apply, it should be interpreted rather narrowly as the requirement of facilitation (Art. 12(2)) and the obligation of maintaining a record of processing activities (Art. 30(1)) create a responsibility on the side of the controller to enable the execution of each individual's rights, as well as control the involved dataflows.[863] Impossibility could, however, be given where a receiving entity was no longer in business and did not have a legal successor.[864] When assessing the proportionality of the required effort, on the other hand, the overall circumstances including the criticality of the data and the interests of the individual should be accounted for[865]

Article 17(2) also introduces another notification requirement for controllers where they have made the information in question public. Under such circumstances, the recipient of an erasure request should take reasonable steps to inform other controllers of the data subject's demand. This should also include "any links to, or copy or replication of, those personal data". This constitutes a significant burden for companies since tracing back all possible channels through which the data could have been spread past publication is virtually impossible.[866] In that sense, controllers are urged to carefully consider the necessity and consequences of making personal information publicly available. The question to what extent certain steps

---

[863]Eßer/Kramer/von Lewinski / *Stollhoff*, Art. 19, para 14; Ehmann/Selmayr, *Kamann/Braun*, Art. 19, para 14. Supporting a slightly different view seems to be: Kuner and others / *González Fuster*, Art. 19, 492, 495, as she underlines the fact that the record of processing activities only needs to contain information regarding the "categories of recipients", not specific recipients as such.

[864]*Piltz*, 10 K&R 2016, 629, 633; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 17 DSGVO, para 10.

[865]*Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 17 DSGVO, para 10; Kühling/Buchner / *Herbst*, Art. 19, para 9; Eßer/Kramer/von Lewinski / *Stollhoff*, Art. 15, para 15.

[866]*Hornung/Hofmann*, 68 JZ 2013, 163, 167; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 17 DSGVO, para 27.

might still be considered “reasonable” should be based on the available technology and the costs of implementation. To this end, providers of search engines would most likely be required to notify website owners.[867] Since there are, however, practical limitations to the extent to which providing information to third parties can be practically achieved by controllers, *often* thorough notification will in fact not lie within the realm of reasonable expectancy. In that sense, the above described Data Revocation Service would in fact constitute an immense improvement when it comes to controlling one’s personal data.

d) Interim Conclusions: Erasure

This right for erasure enables individuals to have information concerning them removed and thereby constitutes a central part of gaining control over one’s personal data. Additionally, to its overall importance in the context of the idea of informational self-determination, it also serves the objectives of multiple principles of data protection, such as purpose limitation, data minimisation, storage limitation, integrity, and confidentiality. The grounds for its application can either occur automatically (e.g., data is no longer necessary for the original purpose, legal requirement for erasure) or be based on a request of the data subject (e.g., objection, withdrawal of consent). There are also, however, a number of exemptions which need to be accounted for prior to fulfilling a deletion request. While some are relatively straight-forward (e.g., compliance with legal obligation), others, such as exercising the right of freedom of expression and information or archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, create the need for multiple fundamental rights and freedoms to be weighed against each other and balanced against the interests of various parties. While the support of a third-party intermediary in that regard should

---

[867] Schwartmann/Jaspers/Thüsing/Kugelmann / *Leutheusser-Schnarrenberger,* 'Art. 17' DSGVO, para 52.

be considered a welcome enhancement, such an entity would not fall under the definition of a Personal Information Management System.

Additionally, to these struggles in legal interpretation, controllers looking to comply with erasure requests are *often* also confronted with a number of technical and organisational obstacles. For example, long-term back-up solutions aimed at the archiving of an organisation's history of records *often* pose a considerable practical obstacle. Whereas PIMS will most likely not be able to solve the inherent problems of any data deletion policy, they might be able to further the overall interest of the data subject through features such as the possibility of request specification or check-lists provided to controllers, as these would assure more transparency as to the factual outcome of the individual's request. There are also a number of solutions being proposed in the context of enabling data deletion on the internet. These mainly relate to the creation of expiration dates for specific datasets and the facilitation of retrospective data revocation. Data Revocation Services, based on the use of unique data identifiers which allow the creation of push and pull notices to controllers, could also be further applied for the purpose of submitting such requests to all relevant parties at once. This would directly support controllers in their obligations enshrined in Article 17(1) and Article 19, while simultaneously strengthening the rights and freedoms of individuals and allowing them an unprecedented degree of control over their personal data.

4. Restriction

The right to restriction of processing enshrined in Article 18 of the GDPR constitutes a new right in the realm of data privacy. While Art. 12(b) of the Data Protection Directive did mention the possibility of "blocking" data where its processing did not comply with the law, both its nature and implications were largely unclear.[868] The implementation of blocking under the old German BDSG in §§ 20(3)(7) and 35(4)

---

[868]Kuner and others / *González Fuster*, Art. 18, 485, 487; Schwartmann/Jaspers/Thüsing/Kugelmann / *Keber/Keppeler,* 'Art. 18' DSGVO, para 2f.

Nr. 4 was, for example, considered as a milder device in comparison to erasure but was not seen as a separate right.[869]

a) Grounds for Application

Article 18(1) provides for four instances under which data subjects can require restriction of the processing of personal data from the controller. First of all is the case where there are doubts regarding the accuracy of personal data (Art. 18(1)(a)). Here processing should be restricted until such has been verified. This time period should however in principle be very limited, since controllers have a direct obligation to rectify data without undue delay in accordance with Art. 16 and to take "every reasonable step" to ensure erasure or correction of incorrect information based on Art. 5(1)(d).[870]

The second ground for application refers to instances where no legal basis for the further processing of personal data exists, however, the data subject requests its restriction rather than erasure. Logically, this would most likely concern cases where individuals could request the erasure of data under Art. 17(1)(d), but would prefer to refrain from such an irreversible measure.[871] This might, for example, make sense when the individual wished to further inquire as to the extent of the processing which took place unlawfully, thereby following similar interests as Art. 18(1)(c).[872] The data subject is, however, not required to provide any reasoning for their choice, neither is the right subject to any time limit.[873] In that sense, the decision of the individual can inadvertently create a substantial burden for the controller. While the principles of data minimisation and storage limitation have the primary purpose of protecting the

---

[869]Eßer/Kramer/von Lewinski / *Stollhoff*, Art. 18, para 1f.

[870]Kuner and others / *González Fuster*, Art. 18, 485, 489; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 18 DSGVO, para 4f.

[871]Kuner and others / *González Fuster*, Art. 18, 485, 489.

[872]*Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 18 DSGVO, para 6f; Eßer/Kramer/von Lewinski / *Stollhoff*, Art. 18, para 17.

[873]Ehmann/Selmayr, *Kamann/Braun*, Art. 18, para 17; *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 18 DSGVO, para 6.

data subject, they also have indirectly led to a minimisation of risks on the side of the controller, who otherwise needs to ensure appropriate technical and organisational measures for the protection of the restricted data for a prolonged period of time.

Restriction of processing can also be required when the information is no longer necessary for the original purpose of the processing but the data subject needs it for the establishment, exercise or defence of legal claims. This exemption should be interpreted similarly to Art. 17(3)(e). In that sense, while it would not be necessary for an actual legal procedure to be in progress, the data subject should be able to demonstrate a sufficient probability of the occurrence of a legal claim in the near future.[874] The applicability of the right to restriction is therefore significantly more limited than under Art. 18(1)(b), since the controller will conversely have the right to erase the data in question once the data subject can no longer assert the existence of a legal interest or where the proceedings in question have been finalised.[875]

Finally, the restriction of processing might be warranted where an individual has filed an objection to the processing in accordance with Art. 21(1) GDPR but the controller, however, is arguing the existence of overriding legitimate grounds for the continuation of the processing. Such an objection can be filed where the processing is based on the controller's legitimate interests (Art. 6(1)(f)) or is necessary for tasks carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(e)).[876] As long as the existence of overriding grounds on the side of the controller is verified, the processing operation should be put on hold. In accordance with Recital 69, the burden of proof for demonstrating such

---

[874]Wolff/Brink/v. Ungern-Sternberg / *Worms*, Art. 18 DSGVO, para 41; Paal/Pauly / *Paal*, Art. 18 DSGVO, para 18; Kühling/Buchner / *Herbst*, Art. 18, para 22f.

[875]Wolff/Brink/v. Ungern-Sternberg / *Worms*, Art. 18 DSGVO, para 41; Ehmann/Selmayr, *Kamann/Braun*, Art. 18, para 20; Kuner and others / *González Fuster*, Art. 18, 485, 491.

[876]Kuner and others / *González Fuster*, Art. 18, 485, 490.

should be put on the controller.[877] Similarly to Art. 18(1)(a), the time period for which the processing will be restricted should be limited in this instance, as it should only apply as long as the legitimacy of the processing is being verified.[878] Once this is completed, the processing will either continue based on the overriding interests of the controller, or the data should be deleted in accordance with the wishes of the data subject.

b) Consequences and Modalities

Once the existence of a valid request for the restriction of processing has been confirmed, the question occurs through which modalities this could be implemented by the controller. Article 4 No. 3 of the GDPR defines restriction of processing as "marking of stored personal data with the aim of limiting their processing in the future". Article 17(2), on the other hand, does not mention the marking in any way but focuses mainly on the fact that the only legitimate processing activity which should be taking place (given the absence of the applicability of an exception) is storage. A little more insight into the possible practical procedures, which could be used in order to facilitate the implementation of this right, is given by Recital 67. Here, it is outlined that the methods such as temporarily moving the data in question to another system or making it temporarily unavailable to users, should be considered. Also, information which has been published on the internet should naturally be removed from the website.

The mentioned examples clearly Indicate that controllers are required to put in place appropriate technical and organisational measures that effectively hinder any further processing of personal data. In that sense, only "marking" the data without the implementa-

---

[877] *Voigt/von dem Bussche*, GDPR, 178.

[878] Gola/Heckmann / *Gola*, Art. 18 DSGVO, para 19; Kühling/Buchner / *Herbst*, Art. 18, para 27; Ehmann/Selmayr, *Kamann/Braun*, Art. 18, para 23; Kuner and others / *González Fuster*, Art. 18, 485, 491.

tion of any other controls would most likely not be considered sufficient.[879] Instead, it should be assumed that to the extent possible, any sort of access to the data should be made impossible, either by moving its physical location or completely blocking any respective rights within a system.[880] In the case of automated filing systems, Recital 67 also postulates that the possibility of restricting certain datasets from further processing or adjustments should in principle already be employed within the architecture. This is in line with the principle of data protection by design and default, which calls for the integration of necessary safeguards into any system per default (Art. 25 GDPR).

While the requirement of including the possibility of data restriction within any given system per default is absolutely reasonable and in line with current technical standards, controllers are unfortunately still confronted with the existence of legacy systems which cannot be deployed but also do not contain the necessary functionalities.[881] In that sense, the controllers will be forced to consider the implementation of interim solutions since Article 18 does not provide for any exemptions based on disproportionate effort or practical impossibility. In that context, the involvement of a Personal Information Management System in the process of restricting the processing of personal data might be considered an interesting alternative.

c) Involvement of PIMS

In comparison to other rights and obligations found in the GDPR, the right to the restriction of processing has so far not received wide attention, both in the context of policy debates, as well as academic

---

[879]Ehmann/Selmayr, *Kamann/Braun*, Art. 18, para 27; Kühling/Buchner / *Herbst*, Art. 18, para 30.

[880]Ehmann/Selmayr, *Kamann/Braun*, Art. 18, para 27; Kühling/Buchner / *Herbst*, Art. 18, para 30; *Piltz*, 10 K&R 2016, 629, 633.

[881]For more on the issue see for example: *Al-Ali and others*, in: ECSA '19, 277, 277ff; *Márquez and others*, in: Advanced Information Systems Engineering, 507, 507ff.

literature.[882] This presumed lack of interest might in part be based on the fact that the explicit regulation of such a right has been newly introduced by the GDPR, due to which there was not much room for debate prior to its coming into force. Also, the right might seem relatively "tame" and is certainly subject to fewer controversies than rights such as erasure or access.

aa) Considerations on the Market Realities

The general lack of attention given to this particular right, which in turn leads to a certain "unmarketability" of services offering its provision, is most likely also the reason why the right to restriction does not seem to be the focus of developers of Personal Information Management Systems at present. In fact, at the time of writing, none of the reviewed providers contained any mention of the right to restriction in the meaning of Art. 18 on their websites. The lack of primary focus on this right is to an extent understandable, since the restriction of processing does not really constitute a right in its own merit but rather is contingent on the presence of another privacy relevant modality.

For grounds based on Art. 18(1)(a) and (d), this modality manifests itself in the intention of the data subject to execute another data subject's right, namely the right to rectification or objection, whereas the controller claims the existence of obstacles that hinder them from acting according to the individual's request, either because they consider the data in question to be correct or based on the existence of overriding legitimate grounds for the continuation of the processing. In those instances, the right to restriction only constitutes an interim solution until the underlying conflict between the controller and data subject is resolved and the processing of personal data can be continued (or ended) in an appropriate manner.

Points (b) and (c) of Article 18, on the other hand, are conditional upon the existence of a ground for erasure, namely unlawful pro-

---

[882]Kuner and others / *González Fuster*, Art. 18, 485, 489.

cessing (Art. 17 (1)(d)) or loss of purpose (Art. 17(1)(a)). The difference in comparison to the other two modalities lies in the fact that here, the data subject wishes for the data to be retained for a longer period than anticipated by the controller. The basic principle, however, is the same: a data subject's right conflicts with the wishes of one party to continue the processing of personal data; as a result, a conflict between the involved parties arises and the data shall be processed in a restricted manner until such conflict is resolved.

Considering its inherent dependency on the presence of other data subject rights, the right to restriction in a sense manifests more as an interim compromise between claims, rather than a tool for individuals to take control of the processing of their personal data in its own merit. Against this background, the relative lack of focus of providers of Personal Information Management Systems in advancing the possibilities of individuals to enforce Art. 18 is logically understandable. On the other hand, the potential for improvement should still be examined.

bb) Potentials for Developements

In the underdeveloped potential of Personal Information Management Systems, in this area effectively lies the possibility of taking over the data. As outlined in the proceeding text, the whole basis of restricting the processing has its root in an underlying conflict between the controller and the data subject regarding the further processing of personal data. It should therefore be considered a welcome advancement for the data in question to be stored with a third party until a resolution has been found. Such a solution would, on the one hand, alleviate the controller from the burden of separating and securing the information in order to assure its confidentiality and integrity, while at the same time guaranteeing that no further processing can take place. On the other hand, the data subject would be reassured that no illegitimate activities are taking place while the future status of the information is being clarified.

Similar solutions, in a sense already exist in the area of scientific research. Standardised codes of conduct and guidelines regulating

the management of research data generally oblige scientists to prolonged data retention after the completion of a project or publication.[883] The most common storage period in that context is 10 years;[884] for some types of data, this might, however, be even longer.[885] Considering the potential risks and challenges which can arise as a result of such long-term data retention,[886] the use of specialised data repositories for that purpose is generally advised.[887] While the involvement of a third-party provider for prolonged data retention is not the same as using one for the restriction of processing, the modality of handling the data is, in a sense, similar. Data stored after the completion of a research project, based on the standards of good scientific practice, is not actively being used, it is simply being preserved. The same arguably applies in the case of restriction, as the data is only supposed to be stored, not actively processed in any other manner. It should therefore be imaginable that providers of Personal Information Management Systems could use similar structures for preserving the information of the data subject while it is subject to restriction under Art. 18. Such an extension of the service offering should, in fact, be more or less uncomplicated in

---

[883] *DFG*, Safeguarding Good Research Practice, 22; Association of Universities in the Netherlands, Code of Conduct for Academic, 8.

[884] For example: https://www.stmarys.ac.uk/library/research-support/research-data-management.aspx (accessed: 16 October 2025); https://www.ulster.ac.uk/__data/assets/pdf_file/0006/858345/Research-Data-Management-Policy.pdf (accessed: 16 October 2025); https://www.crick.ac.uk/sites/default/files/2018-07/crick_scientific_research_data_management_policy_0.pdf (accessed 26 February 2026); https://www.southampton.ac.uk/about/governance/regulations-policies/policies/research-data-management (accessed 17 February 2026).

[885] https://www.crick.ac.uk/sites/default/files/2018-07/crick_scientific_research_data_management_policy_0.pdf (accessed 26 February 2026).

[886] *Lefebvre/Bakhtiari/Spruit*, 62 it - Information Technology 2020, 29, 29ff; *Lu/Su*, 2 Open Access Journal of Clinical Trials 2010, 93, 93ff.

[887] *European Commission*, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020 (26 July 2016), 8; *Science Europe*, 'Practical Guide Research Data Management', 25-30; *Schmidt/Kuchma*, Implementing Open Access, 60-88.

instances where secure storage is already part of the provider's service offering.[888]

d) Interim Conclusions: Restriction

Article 18 of the GDPR provides the data subject with the right to restriction of the processing of their personal data in instances where (a) its accuracy is being contested; (b) the processing is unlawful; (c) it is no longer necessary for the original purpose; or (d) an objection submitted to the controller under Art. 21(1) is pending verification. Effectively, this means that the right to restriction only constitutes an interim solution until the underlying conflict between the controller and data subject is resolved. Afterwards, the processing will either continue or be ended through the erasure of the data in question. While supporting individuals in the exercising of their right to restriction is currently not part of the standard service offerings of existing PIMS, there are definitely possibilities of including such which should be explored. The suggested solution would entail the takeover of the data in question for the time of its restriction by the PIMS provider, in order to guarantee its security for that period. This could, in a sense, function analogously to the already established practices of data repositories in the field of scientific research.

5. Portability

The right to data portability has been newly introduced by the General Data Protection Regulation.[889] It essentially follows two main rationales: First of all, data subjects are to be empowered through the ability to easily move, copy, or transmit their personal data and secondly, fair competition between controllers is to be advanced through the facilitation of a free flow of information.[890] Therefore, while the

---

[888]See Part 1 Chapter 2: A. Storage.

[889]*Jülicher/Röttgen/v. Schönfeld*, 8 ZD 2016, 358, 359; *Dehmel/Hullen*, 4 ZD 2013, 147, 153; Kuner and others / *Lynskey*, Art. 20, 497, 500.

[890]*Art. 29 WP,* Guidelines on the right to data portability, 4; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 2f; Kuner and others / *Lynskey*, Art. 20, 497, 499.

requirements under Art. 20 apply to all types of businesses equally,[891] the lawmakers most likely intended them to be aimed at controllers whose underlying business model is based on the collection and processing of personal data.[892]

a) Applicability

Art. 20(1) sets out three conditions for the applicability of the right to data portability: (1) the data has to be provided to the controller by the data subject; (2) the processing needs to be based on consent or performance of contract; and (3) it has to be carried out by automated means.

The Article 29 WP seems to be in support of a wide interpretation of the characteristic of "being provided" by the individual, explicitly including not only information actively submitted to the controller, but observed data, collected through the use of a specific service or device, as well.[893] In order to avoid a boundless expansion of the claim it should, however, be assumed that the component of provision requires the data subject to be conscious of the fact that data is being submitted to the controller and to allow this willingly and knowingly.[894] Information which is being generated by the controller such as inferences or conclusions, is thereby clearly excluded from the claim.[895]

The fact that the right to portability only applies to processing operations based on consent (Art. 6(1) (a) or 9(2)(a)) or performance

---

[891]This fact has been subject to much criticism, pointing out that small and medium sized businesses might be disproportionately burdened by this requirement. See for example: *Vanberg/Ünver*, 8 EJLT 2017, 1, 4; *Graef*, 39 Telecommun. Policy 2015, 502, 506; *Swire/Lagos*, 72 Md. L. Rev. 2013, 335, 351ff.

[892]*Scudiero*, 3 EDPL 2017, 119, 119 and 122; *Jülicher/Röttgen/v. Schönfeld*, 8 ZD 2016, 358, 361.

[893]*Art. 29 WP,* Guidelines on the right to data portability, 10.

[894]*Jaspers*, 36 DuD 2012, 571, 573; *Voigt/von dem Bussche*, GDPR, 170; Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 15.

[895]*Strubel*, 8 ZD 2017, 355, 360; *Art. 29 WP,* Guidelines on the right to data portability, 10; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 14; Kühling/Buchner / *Herbst*, Art. 20, para 11.

of contract (Art. 6(1)(b)), is further underlined by Recital 68, which states that it cannot be exercised where processing is being carried out for the compliance with a legal obligation or in the context of a task carried out in the public interest or in the exercise of an official authority vested in the controller. While data subjects also have no legal grounds for demanding a data transfer where the processing is based on legitimate interest (Art. 6(1)(f)), Art. 29 WP still postulates the development of procedures allowing customers to directly access their information *"in a portable, user-friendly and machine-readable format"* as part of their best practices.[896]

Article 20(1)(b) introduces another restriction to the right to data portability, clarifying that it only applies where processing is being carried out by automated means, thereby excluding data processed by other means, forming or intended to form part of a filing system, which would normally be within the material scope of the GDPR in accordance with Art. 2(1). The reason for this limitation can most likely be traced back to the drafting stage of the Regulation, as the idea originally initiated in the context of the information society and internet services.[897] It is also logical from a practical perspective. Since the right to data portability requires data to be submitted in a machine-readable format, the inclusion of paper-based files would additionally have put the burden of reformatting those on the controller. This might be considered disproportionate especially given the relatively lower risk of paper-based processing.[898]

---

[896] *Art. 29 WP,* Guidelines on the right to data portability, 8; *Art. 29 WP*, Opinion 06/2014, 47f.

[897] *Zanfir*, 2 IDPL 2012, 149, 157; Kuner and others / *Lynskey*, Art. 20, 497, 504.

[898] While a well organised paper-based filling system, can still make finding information relatively easy (see for example: *FRA*, Handb. on EDPL, 100), the overall risk which might arise from excessive data cumulation, combination and the creation of inferences significantly lower. The inclusion of paper-based files into the scope of the GDPR, was in fact motivated mainly by the fear of controller circumventing the Regulation (see Recital 15).

b) Modalities

The right to data portability consists of two basic elements: The right of the data subject to receive information directly, and to transmit or have such data transmitted to another controller. These elements can be realised through three forms of action.

aa) Receipt

The most basic form of the right to data portability establishes a right of the data subject to receive the information concerning them, which they have provided to the controller. The right to obtain one's own personal information, however, refers to the possibility of acquiring a copy of such, and not necessarily the dataset originally collected.[899] Otherwise the right to data portability would automatically stipulate a requirement for deletion on the side of the controller.[900] This has, however, been expressly ruled out by Art. 17(3), which states that the exercising of that right should be without prejudice to Art. 17.[901] When it comes to the relationship to other data subject rights, a strong resemblance to the right to receive a copy under Art. 15(3) can also be observed. However, as already outlined under Part 1 Chapter 2: D. II. 1. c) aa) Relationship to Data Portability, the two pursue entirely different purposes. The purpose of obtaining a subset of one's own personal information lies in the possibility of further reusing such and managing it in accordance to one's preferences,[902] whereas the right to access is focused primarily at ensuring that individuals can obtain full disclosure as to the processing of personal data concerning them.[903] Article 20 is also generally considered far

---

[899]*Jülicher/Röttgen/v. Schönfeld*, 8 ZD 2016, 358, 360; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 22; Wolff/Brink/v. Ungern-Sternberg / *von Lewinski*, Art. 20 DSGVO, para 115.

[900]Wolff/Brink/v. Ungern-Sternberg / *von Lewinski*, Art. 20 DSGVO, para 115; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 22.

[901]Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 22; Paal/Pauly / *Paal/Hennemann*, Art. 12 DSGVO, para 23f.

[902]*Art. 29 WP,* Guidelines on the right to data portability, 5.

[903]Kühling/Buchner / *Herbst*, Art. 20, para 4; *Brink/Joos*, 11 ZD 2019, 483, 484.

more specific as it only covers certain types of data processing operations while, on the other hand, requiring a specific format of submission from the controller as well.[904] For PIMS this modality will be most relevant where the system is not qualified as a data controller but rather processor or third party. Here the possibility of having data transferred onto the tool will need to be derived from the individual, with the PIMS being considered as an element of the individual's personal sphere of influence.

bb) Transmission

The focus of the right to data portability, enabling individuals to manage their own personal data, is also evidenced in the second modality of Art. 20(1), namely the right of the individual to transmit the information received to another controller without hindrance. The term "hindrance" should be interpreted widely in that context. Art. 29 WP, for example, defines it as any type of *"obstacles placed by a data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller"*.[905] In that sense, anything that would make the exercise of such a right more difficult could potentially fall under this term including the attachment of any sort of conditions or quality limitations.[906] Typical hindrances could potentially include obstacles of a financial (charging a fee), technical (knowingly transferring data in a format unreadable by other controller), or legal (asking data subjects to sign non-disclosure agreements) nature.[907] It should, however, be noted that this particular modality does not include a requirement to support or in any way

---

[904] *Schätzle*, 2 PinG 2016, 71, 74; Kühling/Buchner / *Herbst*, Art. 20, para 19.

[905] *Art. 29 WP,* Guidelines on the right to data portability, 15.

[906] *Jülicher/Röttgen/v. Schönfeld*, 8 ZD 2016, 358, 359; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 27.

[907] Kühling/Buchner / *Herbst*, Art. 20, para 22; *Art. 29 WP,* Guidelines on the right to data portability, 15; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 27; Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 13.

facilitate the transfer of information to another entity; it solely prohibits the active creation of obstacles, still leaving the burden of performing the actual data transfer on the data subject.

cc) Direct Transmission

Finally, Article 20(2) adds another element to this modality by giving individuals the right to have their data directly transmitted from one controller to another. Depending on the legal classification of the PIMS, it might therefore qualify as "another controller". Also imaginable are instances where a PIMS would conduct the data transmission to a third entity on behalf of the data subject.

This element, while also aiming at the empowerment of the individual, is additionally intended to serve other, more economical purposes as well. On the one hand, enabling an unrestrained, but yet secure flow of information between providers could have the potential of fostering opportunities for innovation.[908] At the same time, the so called "lock-in effect" for consumers should be reduced by facilitating the possibility of switching between providers without having to bear the burden of manually transferring all necessary information by themselves.[909] Although the potential of effortless data portability for the promotion of innovation is undeniable, there are also voices of concern pointing out that such a requirement might cause the opposite effect by potentially supporting anti-competitive conduct in certain markets,[910] as well as putting an unproportionate burden on small and medium enterprises.[911]

While this constitutes a valid concern it should, however, be remembered that in context, Article 20(2) does stipulate that direct transmission should only be required where *"technically feasible"*. As

---

[908] *Art. 29 WP,* Guidelines on the right to data portability, 15; *Gasser/Palfrey*, Breaking Down Digital Barriers, 12-15.

[909] Kuner and others / *Lynskey*, Art. 20, 497, 499; *Zanfir*, 2 IDPL 2012, 149, 152; *Scudiero*, 3 EDPL 2017, 119, 124.

[910] *Engels*, 5 IPR 2016, 1, 10ff.

[911] *Swire/Lagos*, 72 Md. L. Rev. 2013, 335, 353f; *Vanberg/Ünver*, 8 EJLT 2017, 1, 4.

is, however, so often the case with the vague legal terminology contained in the GDPR, the extent of this limitation is still subject to much debate. Some consider the term to incorporate any options which are reasonably possible based on the state-of-the-art.[912] Such an understanding would, however, be inconsistent with the terminology used in other parts of the GDPR,[913] as well as the clarifications found in Recital 68. The Recital further outlines the extent of this limitation by confirming that while controllers are in general encouraged to develop interoperable formats, the right to data portability *"should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible"*. In that sense, some have argued that "technical feasibility" should be made dependent on the technical solutions currently available to the controller,[914] while others are of the opinion that both objective technical standards and the subjective practicability should be taken into account.[915] Either way, the data subject would need to be informed about the reasons impeding the controller from executing a direct transmission in accordance with Art. 12(4),[916] potentially giving them the option to decide on another alternative.

The dilemma of technical feasibility has led to the concern that as long as universal, broadly accepted standards which make systems interoperable and thereby enable direct transmissions of personal data are not available, the right to portability will not produce any practical effect for the data subject.[917] This fear might in fact have actualised itself to a certain extent. While the right to data portability has, from the start, received much interest in literature, a significant

---

[912] *Albrecht*, 2 CR 2016, 88, 93.

[913] Kühling/Buchner / *Herbst*, Art. 20, para 27.

[914] Laue/Kremer / *Kremer*, §4, para 70; Kühling/Buchner / *Herbst*, Art. 20, para 27.

[915] Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 31; Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 29-31; Rücker/Kugler, *Schrey*, D. General conditions, para 671.

[916] *Art. 29 WP,* Guidelines on the right to data portability, 16.

[917] *Scudiero*, 3 EDPL 2017, 119, 124.

practical effect on businesses has not yet been reported.[918] This should not come as a surprise, as studies suggest a general lack of awareness among individuals concerning this particular right.[919] In that context, the advancement of Personal Information Management Systems actually shows a lot of potential in furthering its relevance, by supporting the development of necessary technical standards, as well as increasing user awareness. This potential has also been explicitly been recognised by the Art. 29 WP in their Guidelines of data portability, which state that individuals *"should be enabled to make use of a personal data store, personal information management system or other kinds of trusted third-parties, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required"*.[920]

c) Format

Directly connected to the question of technical feasibility is the issue of the format in which information needs to be transmitted. This will be relevant especially when a data transmission to the PIMS is done for the purpose of further transfers. Article 20(1) provides that data subjects should receive the relevant data in a *"structured, commonly used and machine-readable format"*. Recital 68 additionally adds the requirement for such a format to be interoperable. In order for data to be structured, it would need to be organised and accessible based on certain criteria.[921] Whereas the GDPR does not technically ask for the structuring to be logical or easily understandable to the data subject,[922] the underlying purpose of structuring information in the first place, which is easier readability and re-usability, should

---

[918] https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/ (accessed 26 February 2026).

[919] *Kuebler-Wachendorff and others*, 44 Informatik Spektrum 2021, 264, 266ff.

[920] *Art. 29 WP,* Guidelines on the right to data portability, 16.

[921] Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 68; Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 26.

[922] Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 26.

be considered.[923] In that sense, individuals should have the right to receive an explanation of the structure where it is particularly enigmatic or convoluted for some reason.

The common use of a certain type of format will be based on the current industry standards.[924] The use of such by a market leader is, however, not sufficient to confirm its prevalence if other providers are not using the same.[925] Supporting an understanding where market leaders could dictate the commonality of a format could in fact be quite dangerous, as it has significant potential to further aggravate already existent lock-in effects. Formats subject to licensing should also not be considered appropriate, where the costs of such would be considerable.[926] Otherwise, the transmission of information in such a form could effectively be considered a "hindrance" in the form of an indirect financial obstacle. Also, finding a format that would be both structured and commonly used can be quite challenging from a practical perspective.[927] In that case, it might be most reasonable to provide the data subject with a number of available choices, leaving them the option to determine which format would be most suitable for their purposes.[928]

The term "machine readable" is defined by the EU Glossary as information *"in a data format that can be automatically read and processed by a computer, such as CSV, JSON, XML, etc".*[929] The definition also specifies that such data has to be structured, making the

---

[923] *OECD*, Data portability, 45; *Art. 29 WP,* Guidelines on the right to data portability, 18

[924] *Art. 29 WP,* Guidelines on the right to data portability, 18; Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 26; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 24.

[925] Wolff/Brink/v. Ungern-Sternberg / *von Lewinski*, Art. 20 DSGVO, para 76; Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 72.

[926] Wolff/Brink/v. Ungern-Sternberg / *von Lewinski*, Art. 20 DSGVO, para 77; Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 72.

[927] *Scudiero*, 3 EDPL 2017, 119, 124; Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 72.

[928] *Art. 29 WP,* Guidelines on the right to data portability, 18.

[929] EUR-Lex Glossary, https://eur-lex.europa.eu/eli-register/glossary.html (accessed: 22 October 2025).

first requirement superfluous. While definitely putting a burden on the controller, the determination of this quality is at least easily verifiable, since the operating system of a computer will in most instances automatically recognise whether or not the information can be retrieved.[930]

As already mentioned above, the requirement of interoperability is added to by Recital 68. In the context of European public service delivery, this term is defined as *"the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems"*.[931] Art. 29 WP elaborates in that context that the mention of interoperability found in Recital 68 does not in fact constitute a new and separate stipulation but rather that the conditions under Art. 20(1) regarding the format are there to set the minimal requirement, which serve the overall purpose of enabling the interoperability of formats.[932] In that sense, interoperability is to be seen as the ideally desired outcome, instead of an actual condition.[933] This understanding is further confirmed in the same Recital, which outlines that the creation of interoperable formats is encouraged (not obliged) and that the creation of technically compatible systems is in fact not demanded.

There does, however, seem to be a certain dissonance within Recital 68. Art. 29 WP tries to solve this conflict by presenting interoperability and compatibility as completely separate modalities, explaining that the right to portability aims at the assurance of the first but not the latter.[934] If the requirements in Art. 20(1), however, are

---

[930]Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 26.

[931]EUR-Lex Glossary, https://eur-lex.europa.eu/eli-register/glossary.html (accessed: 22 October 2025).

[932]*Art. 29 WP,* Guidelines on the right to data portability, 17.

[933]Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 77; Kühling/Buchner / *Herbst*, Art. 20, para 27.

[934]*Art. 29 WP,* Guidelines on the right to data portability, 17.

"minimal" but have the goal of achieving interoperability, then in a sense it would become a prerequisite, rather than only an encouraged solution after all.[935] In that context, some scholars have argued that the right to data portability does in fact introduce an obligation for controllers to create a software able to export data from one service to another, also referred to as an "Export-Import Module".[936]

Whereas the practical consequences resulting for controllers from Art. 20 and Recital 68 are at times unclear, the observed dissonance can most likely be explained through the aspirations of the lawmakers. When the GDPR was still in its early stages of development, the general idea of data portability and interoperability had already emerged in the form of both research and commercial projects.[937] Following the experiences with the Data Protection Directive, the GDPR was specifically aiming for longevity through the principle of technological neutrality.[938] It seems possible that in that context, while interoperability was not yet at a sufficient stage of technical development to make it a legal requirement, it was already at the time seen as a viable and desirable solution in the future. In that context, it would make sense to include a general right for individuals to portability in order to avoid completely omitting a subject of great importance for the future, while leaving open the question of interoperable formats and phrasing it more as a future aspiration, rather than a strict obligation. In consequence, the requirements should also be read as relatively fluid and aspirational in consideration of the current technical developments, putting on controllers the burden to export data in a format which meets the outlined standards to the highest (realistically) possible degree.

---

[935] *Scudiero*, 3 EDPL 2017, 119, 120.

[936] *Swire/Lagos*, 72 Md. L. Rev. 2013, 335, 344f; *Scudiero*, 3 EDPL 2017, 119, 120.

[937] *Ursic*, 15 SCRIPTed 2018, 42, 46-48.

[938] Recital 15. Also: *Schmitz*, 4 ZD 2022, 189, 189; *Benecke/Spiecker gen. Döhmann*, '§ 23 Europäisches Datenschutzverwaltungsrecht' in: Verwaltungsrecht der Europäischen Union, para 7f.

d) Extent

As outlined above under Part 1 Chapter 2: D. II. 5. a) Applicability, the right to data portability only applies to data which has been provided to the controller by the data subject. Another limitation of this claim can be found in both in Points (1) and (4) of Article 20. The first states that the data subject only has the right to receive information "*concerning him or her*", meaning that data concerning other individuals, even if provided to the controller by the data subject, will not be covered by the claim.[939] Where, however, information concerning a third party is inextricably linked to the individual's personal data, the right to data portability should in principle still apply.[940] The extent of such will, however, be restricted in accordance with Art. 20(4), which clarifies that such a right should not have an adverse effect on the rights and freedoms of others.[941] The same wording can be found in Art. 15(4) and has already been examined in that context under Part 1 Chapter 2: D. II. 1. d) Access Only. While a clarification analogous to Recital 63 is missing in this case, it can still be assumed that non-privacy related rights, such as the protection of intellectual property or trade secrets, would also be covered.[942]

It should be noted at this point that the portability or in fact any kind of processing of personal data concerning other individuals can constitute a significant legal dilemma in this context, which relates directly to the definition of the roles and responsibilities of the parties involved. In most standardised service offerings used by a natural person, any kind of personal data of third parties processed (saving e-mail addresses of friends in the contact repository, uploading pictures on a private site etc.) will not be subject to the GDPR as it is covered by the household exemption under 2(2)(c) according to

---

[939]Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 41; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 15f.

[940]*Art. 29 WP,* Guidelines on the right to data portability, 10.

[941]Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 17' DSGVO, para 41; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 15f.

[942]*Art. 29 WP,* Guidelines on the right to data portability, 12; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 36; Gola/Heckmann / *Piltz*, Art. 20 DSGVO, para 38.

which the regulation does not apply to any processing *"by a natural person in the course of a purely personal or household activity"*. Where data is being transmitted to other controllers or in fact managed for other purposes than purely personal ones, the presence of an appropriate legal basis for such further processing needs to be considered.[943]

e) Security

Also similarly, as with the right to access and to receive a copy in particular, there are a number of serious security concerns related to data portability.[944] These relate predominantly to the fear of identity fraud and the threat of attacks performed on the data during transmission.[945] The implementation of necessary security measures or identification procedures should therefore not be considered as a "hindrance" in the meaning of Art. 20(1).[946] In that context, the use of standardised authentication procedures, verified through a Personal Information Management System and as described under Part 1 Chapter 2: D. II. 1. b) cc) Perspectives for Advancement, will most likely constitute a significant improvement for all concerned parties, alleviating the threat of fraudulent access and thereby causing a data breach from the controller, while at the same time ideally taking away the burden of being subjected to complex identification procedures from the consumer.

Also, whereas controllers should be able to secure the transfer of data in itself through the use of appropriate encryption techniques, the highest risk is most likely to stem from the user's system, as most individuals will not have comparable technical and organisational measures in place.[947] This risk is also explicitly recognised by Art. 29 WP, which advises controllers to make data subjects aware of the

---

[943] *Art. 29 WP,* Guidelines on the right to data portability, 11.

[944] See Part 1 Chapter 2: D. II. 1. b) ee) Security of the Copy.

[945] *Scudiero*, 3 EDPL 2017, 119, 124-125; Kuner and others / *Lynskey*, Art. 20, 497, 505; *Art. 29 WP,* Guidelines on the right to data portability, 19f.

[946] *Scudiero*, 3 EDPL 2017, 119, 125.

[947] *Art. 29 WP,* Guidelines on the right to data portability, 19.

associated risks and to *"recommend appropriate format(s), encryption tools and other security measures to help the data subject"*.[948] Whereas having controllers provide advice to the concerned individuals is definitely a noble goal, the use of a Personal Information Management System with an appropriate secure storage functionality as outlined under Part 1 Chapter 2: A. III. Security Measures will most likely be far more effective and should therefore be considered both a more appropriate and convenient measure for the mitigation of such risks.

f) Practical Implementation

Unlike other data subject rights such as rectification and restriction,[949] the idea of data portability has actually been subject to wide attention and development from providers of Personal Information Management Systems, as well as other interested parties. The current offerings can generally be divided into commercial solutions, which are being endorsed directly by data controllers and such, which are offered by independent intermediaries and therefore likely come closer to the actual definition of PIMS. For a full understanding of the current market realities and possible functionalities, both forms should, however, be examined.

aa) Controller Endorsed Solutions

The Data Portability Project, which worked on identifying, contextualising and promoting efforts enabling people to reuse their data across interoperable applications, was founded in 2007.[950] The venture quickly gained importance, with representatives of Facebook, Google and Plaxo confirming their membership of the Working Group

---

[948] *Art. 29 WP,* Guidelines on the right to data portability, 19f.
[949] See Part 1 Chapter 2: D. II. 2. Rectification and 4. Restriction.
[950] *Auwermeulen*, 33 CLSR 2017, 57, 58; *Ursic*, 15 SCRIPTed 2018, 42, 46.

by January 2008.[951] As a result, solutions such as "Google Takeout", a tool enabling users to export their data from various Google products into a downloadable, achivable file[952] or the "Download Information Tool" of Facebook, which allows individuals to download a copy of their Facebook information at any time,[953] were developed.

This initiative further evolved into the establishment of the Data Transfer Project in 2018, which during the time of writing has gotten further support from the Data Transfer Initiative.[954] Whereas the previous commercial initiatives were limited to allowing the retrieval of data by the user but largely failed at enabling any kind of meaningful further transfer of information,[955] this new initiative was explicitly aimed at facilitating both the downloading of data, as well as its transfer between services.[956] This functionality is implemented through the use of existing Application Programming Interfaces (API) and authorisation mechanisms to access data, which are then translated through the use of Data Adapters[957] and Authentication Adapters[958] into a common format, and subsequently converted into the API of the recipient service.[959] In order to assure both accessibility and

---

[951] https://techcrunch.com/2008/01/08/this-day-will-be-remembered-facebook-google-and-plaxo-join-the-dataportability-workgroup/?guccounter=1 (accessed: 14 October 2025).

[952] Google Takeout, https://takeout.google.com/settings/takeout (accessed 24 October 2025).

[953] Facebook Help Centre, https://www.facebook.com/help/405183566203254?cms_id=405183566203254&published_only=true (accessed 14 October 2025).

[954] Data Transfer Initiative, https://dtinit.org/ (accessed 14 October 2025).

[955] *Auwermeulen*, 33 CLSR 2017, 57, 58; *Ursic*, 15 SCRIPTed 2018, 42, 47.

[956] Data Transfer Project Overview and Fundamentals, https://dtinit.org/assets/dtp-overview.pdf (accessed: 14 October 2025), 3.

[957] ibid 9: "Pieces of code that translate a given provider's APIs into Data Models used by the Data Transfer Projects".

[958] ibid 10: "Pieces of code that allow users to authenticate their accounts before transferring data out of or into another provider".

[959] ibid 12-14.

transparency, the initiative decided to work with an open-source format code.[960] Examples of use cases considered by the initiative included scenarios such as enabling an individual to save their playlists while switching music service providers; transferring data from a legacy provider to a new one; or direct transfer of pictures from social media to a photo printing service.[961]

When analysing both these functionalities, as well as the purposes outlined by the founders of the initiative, the Data Transfer Project (DTP) would seem to have all the qualities necessary to be considered a Personal Information Management System, at least when using the definition taken as a basis for this thesis (see Part 1 Chapter 1: B. Context of the Thesis). The Opinion of the European Data Protection Supervisor (EDPS) describes such as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*[962] and the same interpretation with minimal variations has been largely deployed within the literature on the subject.[963] Surprisingly, however, the Project does not consider itself as such, specifically mentioning that PIMS and the DTP have overlapping features but clearly separates the two.[964] The differentiation is based on the assumption that PIMS would connect providers though the creation of an additional copy of the individual's

---

[960]ibid 5.

[961]ibid 5f.

[962]*EDPS*, Opinion 9/2016, para 4.

[963]https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht, 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[964]Data Transfer Project Overview and Fundamentals, https://dtinit.org/assets/dtp-overview.pdf (accessed: 14 October 2025), 18.

data, whereas in the DTP, the information in stored within the originating service with destination services receiving a new copy.[965] This factor alone, however, would not be sufficient to deny the DTP the quality of a Personal Information Management System. After all, the EDPS Opinion specifically acknowledges the existence of multiple data storage models within such, stating that while some *"are designed to keep the users' data in a single place; others are creating a logical link among users' data, which may stay with various service providers"*.[966] Also, the DTP does in fact consider the possibility of cooperating with third party hosting entities in addition to their distributed deployment model.[967] If the Data Transfer Project used a different definition of PIMS, such a differentiation might after all be understandable but the project overview explicitly links to the website of the EDPS, thereby seemingly supporting that definition as well.[968]

The reasons for which the DTP attempts to distance itself from the term "Personal Information Management System" are not clear. There might be a potential fear that consumers would not accept an initiative from market players generally known for processing large amounts of personal data and being in constant conflict with Data Protection Authorities, rather than patrons of data privacy and protection. Considering the overall rise in interest in PIMS, the Project might also be concerned about being subject to further scrutiny, if it is marketed as such. These, however, are all theories, with no actual evidence behind them. The underlying motives are also, in a sense, irrelevant. What is crucial in this context is that it again evidences the overall confusion and lack of specification when it comes to the term "Personal Information Management System". After all, can a certain tool with a pre-defined functionality decide whether or not it would be considered a PIMS, based on the creator's preference? Such a result should not only to be considered extremely unsatisfactory from a

---

[965]ibid 18.

[966]*EDPS*, Opinion 9/2016, para 10.

[967]Data Transfer Project Overview and Fundamentals, https://dtinit.org/assets/dtp-overview.pdf (accessed: 14 October 2025), 14.

[968]ibid 19

consumer's perspective, but potentially dangerous as well. The whole idea of the introduction of PIMS onto the market was structuring the overly complex environment of data processing operations in a way more intelligible for the data subjects.[969] If services are, however, free to choose their denomination based on marketing strategies rather than actual functionality, then this already complex environment will become even more perplexing. This problem, as well as potential solutions, should therefore be further analysed in Part 2 of this thesis.

bb) Offerings through Intermediaries

The second type of Personal Information Management Systems are those offered by independent intermediaries. These are also the types of services more typically considered as falling under the definition of PIMS. They are, however, by no means uniform and include a wide range of functions and approaches. In order to provide a general overview and understanding of the current service offerings, as well as those under development, some of these will be presented below.

(1) MyDex

The platform has already been mentioned in the context of consent management, which seems to be its primary focus at the moment.[970] The provider does, however, also declare that it is following the aim of supporting data portability to the highest possible extent

---

[969] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[970] See Part 1 Chapter 2: C. IV. 3. MyDex

as well.[971] As of the time of writing, receiving data already held by a controller was not considered a part of the offered services, however where data was originally provided via the platform, its re-collection, transmission and further distribution would be possible.[972] This can be facilitated through the following elements of the service offering, which have been previously analysed: (1) the Personal Data Store, used for the collection, retrieval, and storage of personal information; (2) the Personal Data Exchange Services, adding the possibility of distributing such between organisations and other parties; (3) the included Platform, enabling two-way engagement between individuals and controllers; and (4) the Web App Generator, providing a tool for transforming manual services into digital applications.[973] The Personal Data Store of each individual is kept independent of any data collection from controllers, which is facilitated through unique and separate encryption keys.[974] The platform itself, however, operates on a "zero knowledge philosophy", with no access to the information.[975]

(2) CozyCloud

The CozyCloud offers four main features.[976] CozyNotes would technically not fall under the definition of a Personal Information Man-

---

[971]MyDex, 'Data Portability White Paper', https://mydex.org/resources/papers/Data_portability_white_paper/mydexcicdataportabilitywhitepaper2018-06.pdfhttps://mydex.org/resources/papers/Data_portability_white_paper/mydexcicdataportabilitywhitepaper2018-06.pdf (accessed: 14 October 2025).

[972]MyDex, https://mydex.org/platform-services/#mrd (accessed: 14 October 2025).

[973]ibid.

[974]MyDex, 'Achieving Transformation at Scale' (April 2021) 9 https://mydex.org/resources/papers/AchievingTransformationAtScale/AchievingTransformationatScaleMydexCIC-2021-04-14.pdf (accessed: 14 October 2025).

[975]idid.

[976]CozyCloud, https://cozy.io/en/features/#synchronise (accessed: 14 October 2025).

agement System, as applied for this thesis, but rather the one outlined under Part 1 Chapter 1: A. I. Organisers, as it simply allows individuals to take notes and collaborate with others on such.[977] CozyPass basically constitutes an authentication mechanism, allowing users to store and synchronise their passwords and credentials in one place, for convenience.[978] CozyBanks constitutes a banking application, providing users with on overview of multiple accounts at once.[979] While this functionality would probably not be considered a classical "Personal Information Management System" at first glance due to its focus on banking, it could still be recognised as such since it includes an overview of the user's complete personal (financial) data, while at the same time allowing control of that data flow. By aggregating information from multiple accounts, it also effectively accommodates data portability, as it needs to collect the personal (financial) data in question from multiple controllers. The final and most relevant feature is called CozyDrive and allows secure storage and sharing of all types of data. It also includes the possibility of importing data from a list of pre-defined providers. While this cannot yet be considered as providing data portability in general, it does constitute an important step into the direction of centralised data management by the concerned individual. It also evidences the already mentioned tendency of PIMS to include multiple functionalities at once, in this case: authentication, storage, consent, and portability.

(3) World Data Exchange

An application which seems to be to a large extent focused on the economic aspects of data portability, World Data Exchange has also already been mentioned in the context of consent management service.[980] The provider facilitates the retrieval and harmonisation of data from a large but pre-defined list of sources in areas such as

---

[977]CozyCloud, https://cozy.io/en/#notes (accessed 22 October 2025).
[978]CozyCloud, https://cozy.io/en/features/#pass (accessed 22 October 2025).
[979]CozyCloud, https://cozy.io/en/features/#bank (accessed 22 October 2025).
[980]See Part 1 Chapter 2: C. IV. 2. World Data Exchange

social media (e.g. Facebook, Instagram, X, Pinterest), medicine (e.g. Icelandic Health System, NHS, Cerner, Epic), finance (e.g. Visa, Mastercard, Barclays, Citi Bank), health and fitness (e.g. Fitbit and Garmin), as well as music and entertainment (e.g. Spotify and YouTube).[981] While the tool can only be used for secure storage after that,[982] users are generally encouraged to share their data via the one of the provider's apps.[983] This could be done for multiple purposes, such as checking one's social media posts for inappropriate content,[984] having an overview of one's financial situation,[985] or accessing one's health records[986]. In that sense, World Data Exchange again facilitates the provision of consent as well as secure storage, in addition to its portability-focused functionality. It can also be considered as supporting transparency, since individuals will most likely gain a better understanding with regard to the data which is being collected and made available to other data controllers.

(4) Citizen.me

Also incorporating the financial aspect but to a larger extent focused on privacy and empowering data subjects is Citizen.me.[987] The "Zero-Party-Data" technology introduced by the provider is supposed to allow companies and organisations to request information directly from the data subject in real time, which is then to be provided in an anonymised form.[988] Portability is supported through the initial gathering of the data into the application.[989] In contrast to the other presented solutions, information is however stored locally on

---

[981]Wolrd Data Exchange Sources, https://digi.me/sources/(accessed 22 October 2025).

[982]World Data Exchange Features, https://worlddataexchange.com/features (accessed 22 October 2025).

[983]ibid.

[984]ibid.

[985]ibid.

[986]ibid.

[987]CitizenMe, https://www.citizenme.com/ (accessed: 22 October 2025).

[988]ibid.

[989]ibid.

the user's device, without any access from the Citizen.me.[990] Similarly to UBDI, however, individuals are subsequently given the option to share their data in exchange for rewards.[991]

(5) Other Tools and General Remarks

Other initiatives working along the same or similar lines include but are not limited to: Dataswyft,[992] Project Locker,[993] ownCloud,[994] DataBox,[995] DataFund,[996] or Personium.[997] Due to the overall similarities, a detailed presentation of all current offerings on the market would be largely superfluous. This is especially the case since the service offerings in the context of Personal Information Management Systems are extremely dynamic, constantly subject to change and further development. In that sense, the presented examples serve rather as a general overview of the tendencies, regarding the functionalities being offered, in order to facilitate further analysis in Part 2 of this thesis.

While the analysed services vary on multiple factors, such as the type of providers personal data can be accessed from, the envisaged further modalities of processing, the type of storage, or the form of authentication, they all have two important characteristics in common. First of all, none of the current solutions is in fact able to provide "complete" data portability in the sense of being able to both receive and further transfer data, independent of the controller. Secondly, none of the solutions focuses solely on the right to data portability. The support of this right is always connected to the provision of other services such as storage, consent management, transparency, and

---

[990]ibid.

[991]ibid.

[992]Dataswyft, https://www.dataswift.io/for-individuals, (accessed: 22 October 2025).

[993]Project Locker, https://www.projectlocker.com/ (accessed: 22 October 2025).

[994]ownCloud, https://owncloud.com/ (accessed: 22 October 2025).

[995]*Chaudhry and others*, in: Critical Alternatives, 1, 1ff.

[996]Datafund, https://datafund.io/, (accessed: 22 October 2025).

[997]Personium, https://personium.io/en/index.html (accessed: 22 October 2025).

identity management. The reasons for this are obvious. After all, any type of data import will naturally have to be followed by a subsequent storing of such data, regardless of how this is achieved. It is also only logical that, in most instances, the collection of data will also be done for the purpose of further use of such, rather than simply saving it.

The explanation for the inability of these systems to assure the complete and exhaustive retrieval and further transfer of one's data are more of a technical than logical nature. As of now, the most relevant hindrance lies in the inconsistencies of formats and interoperability of the various platforms.[998] Based on these limitations, the current systems can mainly aid the right to data portability in the sense of allowing the establishment of control during data transfers from the platform, enabling the re-use of information and facilitating a better understanding of the data flows taking place.[999] Additionally, issues such as a general lack of awareness regarding the right to portability among individuals, hyperbolic discounting, and a lack of trust in these new solutions significantly limit the target audience to a few tech and privacy enthusiasts, rather than constituting a strong business model of services available to the general public.[1000] In that context, the possibility of monetary compensation for one's data actually constitutes the least privacy-friendly but at the same time most marketable functionality.

g) Interim Conclusions: Portability

The right to data portability applies in instances where processing is performed by automated means and is based either on consent or performance of contract. Also, the data has to be provided to the controller directly by the data subject and concern him or her, in order to be subject to acclaim under Art. 20. This right consists of two basic elements: the rights to receipt and to transmission. These elements

---

[998] *Urquhart/Sailaja/McAuley*, 22 Pers Ubiquit Comput 2018, 317, 325.
[999] *Ursic*, 15 SCRIPTed 2018, 42, 76.
[1000] *Urquhart/Sailaja/McAuley*, 22 Pers Ubiquit Comput 2018, 317, 325.

are realised through three actions: Individuals can receive their personal data directly, they are allowed to further transfer it to different entities and, where technically feasible, request the direct transmission from one controller to another. The data transferred to the individual or to another entity should be provided in an interoperable, structured, commonly used and machine-readable format. This requirement creates a number of practical difficulties in the implementation of the right for controllers. Also, similarly as with the right to access and to receive a copy, the claim is the cause of a number of potential security concerns in relation to the risk of identity fraud, as well as potential attacks performed on the data during transmission.

Considering the multiple practical hurdles which arise as a consequence of the implementation of the right to data portability, a number of service offerings attempting to alleviate these issues have developed on the market. These can generally be divided into commercial solutions which are being endorsed directly by data controllers and such which are offered by independent intermediaries. For the first, the most relevant initiative to be considered is the Data Transfer Project (DTP), which aims at facilitating both the downloading of data as well as its transfer between services. Currently contributing to the initiative are tech giants such as Apple, Meta, Microsoft, Google and X. While the DTP possesses all the qualities necessary in order to fall under the definition of a Personal Information Management System, the Project attempts to distance itself from the terminology.

While there are a large amount of tools on the market being offered by third party intermediaries, none of these have the capability to assure data portability to the full extent, mainly due to inconsistencies in format and lack of interoperability between different platforms. They are, however, to a large extent capable of allowing individuals to control their data transfers and facilitate a better understanding of the occurring data flows. It should also be noted that the current PIMS offerings on the market, which have been analysed above, never solely focus on the assurance of portability but rather do so in addition to other service offerings such as secure storage solutions, consent and identity management, or the transparent display of data

flows. In that sense, they also support the exercise of other data subject rights such as access, rectification, erasure and objection.

6. Objection

Article 21 provides the data subject with the right to object to processing operations performed based on the legitimate interest of the controller (Art. 6(1)(f) GDPR) or on the necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in such (Art. 6(1)(e) GDPR). An objection has to be based on grounds relating to the particular situation of that individual. This claim is often compared with the right to withdrawal laid down in Article 7(3), since both effectively aim at putting an end to a specific processing activity.[1001] While both are in a sense different sides of the same coin and are directed at stopping the processing of personal data, based on a different legal basis, there are two main differences between them. First of all, in the cases of Article 7(3) the processing activity could not have been initiated without the prior consent of the data subject, whereas processing based on points (f) and (e) of Article 6(1) could already be ongoing, without the individual's knowledge.[1002] Also consent can be withdrawn at any time and without any conditions, whereas in the case of objection, the interests of the natural person can be weighed against those of the controller.[1003]

a) Applicability

Article 21 provides for a number of conditions, necessary for its applicability, as well as multiple exceptions. These formal elements of the right to objection will be analysed in the subsequent passages.

[1001] Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 517; Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 3.

[1002] Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 517.

[1003] Paal/Pauly / *Martini*, Art. 21 DSGVO, para 2a; Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 517.

aa) Particular Situation

Data subjects can submit an objection to processing under Art. 6(1)(f) or (e) at any time where such processing cannot be considered legitimate, based on their particular situation. These special circumstances will most likely relate to the weighing of interests, which is being routinely performed for these legal basis of processing.[1004] The individual can therefore bring forward reasons for which the performed analysis of proportionality is not accurate when taking into account their specific circumstances.[1005] Some are in support of a restricted understanding of the term "particular situation", arguing that it should only be considered relevant where absolute rights such as a danger to life or property are affected or where the processing could lead to pressure in ethical, social or family relations.[1006] Such an understanding is, however, not backed by the wording used within the Article, which seems to support a high standard from the grounds demonstrated by the controller, as they need to be "compelling", rather than putting any special requirements on the claim of the data subject. In that sense, it should be assumed that the grounds relating to the particular situation of the data subject would simply need to concern circumstances which were not taken into account during the initial weighing of interests but have the potential to change its outcome.[1007] Should this be confirmed, Art. 20(1) puts an obligation on the controller to cease the further processing of the individual's personal data. This, however, only applies to the information relating to this particular person. The overall processing activity, for which a legitimate weighing of interests has been performed, can on the other hand, still continue.

[1004]Ehmann/Selmayr / *Heberlein*, Art. 6, para 46-53; Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 23, 29ff; Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 55ff.

[1005]Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 19f; Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 9f; Kühling/Buchner / *Herbst*, Art. 21, para 15; LG Frankfurt, ZD 2019, 467, para 32.

[1006]Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 10.

[1007]Kühling/Buchner / *Herbst*, Art. 21, para 15; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 10; Paal/Pauly / *Martini*, Art. 21 DSGVO, para 30f.

bb) Compelling Legitimate Grounds

While controllers are in principle required to cease the processing of personal data where an individual has put forward a valid objection to such, they have the possibility to counter the data subject's claim by demonstrating "compelling legitimate grounds". Such grounds can either be based on the fact that the purpose of processing on the side of the controller overrides the interests, rights, and freedoms of the data subject or that the continuation of such is necessary for the establishment and exercise of defence of legal claims. While the second exception is rather unambiguous and has also already been discussed in other contexts,[1008] the first does leave an extensive amount of room for interpretation.

Considering the requirement for grounds on the side of the controller to be "compelling", it should be assumed that a simple outweighing as a result of the balancing of interests would not be sufficient.[1009] In that sense, the contrary interests at stake would need to override those of the data subject in a substantial, significant way.[1010] It should also not be considered sufficient for the controller to demonstrate the accuracy of the previously performed weighing exercise; rather new reasons which have not been considered before need to be brought forward.[1011] On the other hand, the overriding interests do not necessarily need to relate to the controller as the existence of a general public interest or an effect on the rights and freedoms of third parties are equally imaginable.[1012] Important to note in this context is the fact that the burden of proof, with regard to the existence of such overriding interests, lies on the side of the controller. This

---

[1008]See for example Part 1 Chapter 2: D. II. 3. b) aa) Applicability and Practical Hurdles.

[1009]Laue/Kremer / *Kremer*, §4, para 75.

[1010]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 517; *Art. 29 WP*, Guidelines on Automated individual decision-making, 19.

[1011]*Art. 29 WP*, Guidelines on Automated individual decision-making, 19; Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 13.

[1012]Paal/Pauly / *Martini*, Art. 21 DSGVO, para 36; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 25.

implication results from Art. 20(1), which states that the controller needs to "demonstrate" the existence of compelling legitimate grounds, and is further supported by Recital 69.[1013]

cc) Direct Marketing

Articles 20(2) and (3) provide partially separate rules for cases where an individual objects to the processing of personal data for the purposes of direct marketing. For such instances, Paragraph 2 simply states that data subjects have the right to do so at any time, whereas Paragraph 3 outlines that where an objection has been submitted, personal data should no longer be processed for such purposes. In that sense, none of the conditions mentioned previously, such as the requirement for the existence of grounds relating to the particular situation of that individual or the need to consider compelling legitimate grounds overriding the interests of the data subject, apply.[1014] Based on this, the right to object to direct marketing is also referred to as a "privileged right to object".[1015]

It should, however, also be noted that, in contrast to Paragraph 1, Paragraph 3 does not create a requirement on the side of the controller to completely cease the processing of the individual's personal data. It only obligates the business to stop using it for the purposes of direct marketing, which means that further processing of the relevant information in another context will still be legitimate.[1016] Particularly relevant from a practical perspective is the question to what extent controllers are allowed to keep Blacklists of individuals who previously objected to processing in order to assure that they are not

---

[1013]Kühling/Buchner / *Herbst*, Art. 21, para 22; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 26.

[1014]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 518; *Art. 29 WP*, Guidelines on Automated individual decision-making, 19; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 44.

[1015]Paal/Pauly / *Martini*, Art. 21 DSGVO, para 47.

[1016]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 518; Paal/Pauly / *Martini*, Art. 21 DSGVO, para 52.

again contacted at another point in time.[1017] The Information Commissioner Office at least seems to be in support of such a solution, stating that *"[i]f someone no longer wants you to use their information for direct marketing purposes, you should put their details onto a suppression or 'do not contact' list, instead of deleting them. Doing this means you can check against your list so you don't use their information for direct marketing in future by mistake"*.[1018]

dd) Scientific and Historical Research, Statistics

Article 20(6) also establishes a special set of rules which apply in cases where personal data is being processed for purposes of scientific or historical research or statistics in accordance with Article 89(1). Here the data subject is still granted with the right to object, based on specific grounds applicable to their situation. However, where the processing is necessary for *"the performance of a task carried out for reasons of public interest"*, the claim does not apply. This exemption again demonstrates the significance and, to a certain extent, privileged status given to those purposes by the Regulation.[1019] Since the Article does not require a "demonstration" of such a necessity, some sources argue that this suggests a reversal of the burden of proof.[1020] The prevailing opinion, however, seems to opt against such an understanding.[1021] Also, while the threshold for rejecting an objection might be lower than under Article 20(1),[1022] alternative means of achieving the same purpose with a lesser impact on

---

[1017]Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 23; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 26; Kühling/Buchner / *Herbst*, Art. 21, para 32a.

[1018]*ICO*, 'Direct marketing - detailed guidance'.

[1019]Kühling/Buchner / *Herbst*, Art. 21, para 46; *Chico*, 128 Br. Med. Bull. 2018, 109, 110; *Becker and others*, 30 EJHL 2023, 129, 145-151; *Rossnagel*, 4 ZD 2019, 157, 159; *Weichert*, 1 ZD 2020, 18, 18ff; *Johannes/Richter*, 41 DuD 2017, 300, 300ff.

[1020]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 519.

[1021]Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 66; Paal/Pauly / *Martini*, Art. 21 DSGVO, para 60; Eßer/Kramer/von Lewinski / *Kramer*, Art. 21 DSGVO, para 42.

[1022]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 519.

the rights and freedoms of the data subject, for example through the use of anonymisation or pseudonymisation, should be considered.[1023]

b) Forms of Exercise

In principle, the same formalities as for any other data subject right, which have been outlined in Article 12 of the GDPR and under Part 1 Chapter 2: D. I. Universal Considerations, apply. It should, however, additionally be noted that the objection will, except where it concerns direct marketing, create the need for a declaration from the individual regarding the specific grounds relating to their particular situation.[1024] While there are no requirements as to the format of such, the submission in a written form is generally advisable for documentation purposes, especially taking into consideration the deadlines applicable to the controller.[1025] It should also be remembered that under the requirement of facilitation, controllers have the obligation to establish appropriate channels of communication through which individuals can contact them and put forward their request.

Additionally, to these general requirements, Article 21(5) obliges controllers to create a special type of communication channel in the context of information society services.[1026] Where such are concerned, the data subject should additionally be given the opportunity to exercise the right to object by *"automated means using technical specifications"*. This might, for example, be facilitated through such modalities as "opt-out" links in e-mails or cookie banners or even

---

[1023]Eßer/Kramer/von Lewinski / *Kramer*, Art. 21 DSGVO, para 42; Paal/Pauly / *Martini*, Art. 21 DSGVO, para 60; Kühling/Buchner / *Herbst*, Art. 21, para 54.

[1024]*Franck*, 3 RDV 2016, 111, 113; Kühling/Buchner / *Herbst*, Art. 21, para 56; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 35.

[1025]Kühling/Buchner / *Herbst*, Art. 21, para 56; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 38; Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 520.

[1026]In accordance with Artcile 4 No. 25 GDPR the term information society service means "*a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council*".

providing a special Wi-Fi network for users of mobile phones who do not want to be tracked while passing monitored areas.[1027] Also *often* considered in this context is the possibility of setting up Do-Not-Track features for web browsing activities,[1028] especially in relation to data processing and analysis for the purpose of online advertising.[1029]As those fall under the general term of Privacy Enhancing Technologies, the possibility of their use should also be discussed in the context of Personal Information Management Systems in the subsequent text.

c) Involvement of PIMS

While there are no "classical" problems which can be aided, as was the case with other modalities such as transparency, access or erasure, there is most certainly still room for improvement or at least considerations for such. Since the actual management of a declaration of objection will in principle require an analysis of the individual's particular situation, as well as the consideration of any overriding interests or legal claims which might occur, there is little room for the involvement of a Personal Information Management System at that level.[1030] The involvement of a PIMS is, however, imaginable at both the preceding and subsequent stages, namely in the context of submitting such a request and in connection to the implementation of the consequences arising as a result of such.

[1027]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 519.

[1028]*Albrecht*, 2 CR 2016, 88, 93; *Schantz*, 26 NJW 2016, 1841, 1846; *Caspar* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 21 DSGVO, para 33f; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 66; Kühling/Buchner / *Herbst*, Art. 21, para 43.

[1029]*Cheng/Wang*, 19 JBEM 2018, 253, 253ff; *Kamara/Kosta*, 6 IDPL 2016, 276, 276ff.

[1030]As outlined under Part 1 Chapter 2: D. II. 3. b) bb) Reflections on Potential Advancements: The engagement of a qualified third party into the process of managing assessment, which require the balancing of multiple interests, including those of the data subject and the controller, is in principle a promising idea, but could technically not be included into functionalities offered by PIMS.

aa) Submission

The modalities of submitting a data subject request under Article 21 will vary where the processing activity is being performed for different purposes. As outlined earlier, an objection to processing for direct marketing purposes is to a certain extent privileged and does not require an explanation from the data subject. However, where the individual wishes to object to processing activities which aim at the realisation of other objectives including scientific and historical research or statistical purposes, a declaration from the data subject explaining their particular situation will be necessary.

(1) General Objections

With regard to submitting a request under Article 21(1) and (6), which both require a declaration from the individual as to the grounds relating to their particular situation on which the objection is based, the possibilities of support through a PIMS are to a certain extent limited. Since the reasons for which a processing activity would not be considered as proportionate for a particular person or need to relate to a specific action of the controller, there is very little room for multi-controller submissions, discussed, for example, in the context of rectification or erasure requests[1031] unless they referred to very similar types of processing performed by multiple businesses. The previously considered possibility of request specification, in the sense of drop-down options allowing the person to specify their intent,[1032] can also not be considered appropriate, as grounds relating to an individual's particular situation can hardly be pre-defined and if they were, serious doubts regarding the validity of such an objection could be raised. On the other hand, general features such as the implementation of standardised identification procedures or the automatic calculation of deadlines[1033] could still be deployed for the users' convenience.

[1031]See Part 1 Chapter 2: D. II. 2. b) Multi-Controller Submissions and D. II. 3. c) cc) Multi-Controller Submissions.

[1032]See Part 1 Chapter 2: D. II. 1. c) cc) Request Specification.

[1033]See Part 1 Chapter 2: D. II. 2. b) cc) Perspectives for Advancements.

(2) Direct Marketing

While the possibilities of enabling individuals to exercise their right to objection through Personal Information Management Systems are to a certain extent limited in most contexts, there are special opportunities which arise in which processing is performed for the purposes of direct marketing. Since Art. 21(2) allows for an objection to be submitted without the need to assert any specific reasoning behind such and Paragraph 3 stipulates that where this is the case, the information in question should automatically be excluded from any type of further processing for such purposes, the administrative burdens when it comes to exercising this right are significantly lower. In turn, more or less automated and generalised, multi-controller submissions of objections are allowed, especially since Art. 21(5) specifically stipulates a requirement for controllers to allow the exercise of this right though automated means using technical specifications.

(a) Do-Not-Track

In that context, the implementation of a so-called "Do-Not-Track" functionality should be considered. The idea behind such refers to an automated communication of the system towards the controller's website, that the data subject does not agree to the tracking of their online behaviour for advertising (or other) purposes.[1034] Such a feature is of particular interest to consumers when considering the persistent and excessive amount of personal data collected and analysed by businesses for the purpose of providing personalised online advertising.[1035]

The concept originally initiated in the US, where a number of consumer protection organisations and privacy advocates such as the Electronic Frontier Foundation, the Privacy Rights Clearinghouse,

---

[1034] *Fairfield*, 11 Nw. J. Tech. & Intell. Prop. 2013, 575, 580; *Kamara/Kosta*, 6 IDPL 2016, 276, 276; *Cheng/Wang*, 19 JBEM 2018, 253, 257.

[1035] *Estrada-Jiménez and others*, 100 Comput. Commun. 2017, 32, 32ff; *Bashir/Wilson*, PoPETs 2018, 85, 85ff; *Cooper and others*, 40 JCM 2023, 235, 235ff; *Evans*, 23 JEP 2009, 37, 37ff.

and the World Privacy Forum submitted a list of proposed advancements for "Consumer Rights and Protections in the Behavioral Advertising Sector" to the Federal Trade Commission.[1036] One of the suggested points of action proposed the creation of a "Do Not Track List", similar to the already existent "Do Not Call List".[1037] The proposal also recommended that companies providing browser applications should offer functionalities in the form of a browser feature, extension, plug-in or other, which would allow individuals to create and use a list of domain names to be blocked from tracking their activities.[1038]

Various approaches have since then been taken including ideas such as the creation of a permanent opt-out cookie,[1039] tracking protection features allowing the creation of blacklist and whitelists of websites,[1040] or a HTTP header field sending out signals to website advertisers,[1041] all of which came with their own set of technical constraints and practical implementation issues.[1042] Following this growing interest from industry, the FTC,[1043] lawmakers,[1044] and legal scholars,[1045] the World Wide Web Consortium formed the Tracking

---

[1036] https://cdt.org/wp-content/uploads/privacy/20071031consumerprotectionsbehavioral.pdf (accessed 29 January 2026).

[1037] https://cdt.org/wp-content/uploads/privacy/20071031consumerprotectionsbehavioral.pdf (accessed 29 January 2026). A National Do Not Call Registry, managed by the FTC, contains a list of consumers who do not wish the receive telemarketing calls: https://www.donotcall.gov/ (accessed: 16 March 2026).

[1038] https://cdt.org/wp-content/uploads/privacy/20071031consumerprotectionsbehavioral.pdf (accessed 29 January 2026).

[1039] Google Analytics Opt-out Browser Add-on, https://tools.google.com/dlpage/gaoptout?hl=en (accessed: 14 April 2026).

[1040] *Kuhlmann*, 22 DePaul J. Art, Tech. & Intell. Prop. L. 2011, 229, 279.

[1041] http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html (accessed: 25 February 2026).

[1042] *Kuhlmann*, 22 DePaul J. Art, Tech. & Intell. Prop. L. 2011, 229, 277-282.

[1043] *FTC*, Protecting Consumer Privacy.

[1044] *Tene/Polonetsky*, 13 Minn. J.L. Sci. & Tech. 2012, 281, 319-332.

[1045] *Fairfield*, 14 Vanderbilt J. of Ent. and Tech. Law 2012, 545, 587-601; *Kirsch*, 18 Rich. J.L. & Tech 2011, 1, 2.

Protection Working Group in 2011.[1046] In spite of an impressive list of participants including experts from Microsoft, the Electronic Frontiers Foundation, eBay, Adobe, Google, Apple, The Future Privacy Forum, and Stanford University,[1047] the group, however, failed to make any substantial impact and was closed in January 2019,[1048] citing insufficient deployment and support as part of the reasons.[1049] In 2020, the Global Privacy Control initiative began working on the same objective.[1050] They are offering a browser-level signal, maintained either by a browser or browser extension, which communicates privacy preferences towards the websites.[1051] As of the time of writing, however, only a limited amount of browsers have agreed to adopt the control.[1052]

Additional to the practical issues in implementation is, however, also a significant legal obstacle, at least from the European point of view, hindering the efficient use of these technologies. This is already partially implied on the Global Privacy Control (GPC) website which stipulates that *"the intent of the GPC signal is to convey a general*

[1046] *Kamara/Kosta*, 6 IDPL 2016, 276, 281ff.

[1047] https://www.w3.org/groups/wg/tracking/former-participants (accessed: 16 March 2026).

[1048] https://www.w3.org/2011/tracking-protection/ (accessed: 16 March 2026).

[1049] https://w3c.github.io/dnt/drafts/tracking-dnt.html (accessed 25 February 2026).

[1050] https://iapp.org/news/a/is-gpc-the-new-do-not-track/ (accessed: 25 February 2026); https://www.washingtonpost.com/technology/2021/10/26/global-privacy-control-firefox/ (accessed: 04 March 2026); https://www.wired.com/story/global-privacy-control-launches-do-not-track-is-back/ (accessed 22 October 2025); https://techcrunch.com/2020/10/07/tech-publisher-coalition-backs-new-push-for-browser-level-privacy-controls/ (accessed: 25 February 2026).

[1051] https://globalprivacycontrol.org/Implementing%20GPC%20for%20Publishers.pdf (accessed: 25 February 2026.

[1052] At the time of writing the following browsers are supporting the initiative according to their website: Abine, Brave Privacy Browser, Disconnect, DuckDuckGo Privacy Browser, Firefox, OptMeowt by privacy-tech-lab and Privacy Badger by EFF and lockrMail by lockr. See: https://globalprivacycontrol.org/#download (accessed: 16 March 2026).

request that data controllers limit the sale or sharing of the user's personal data to other data controllers (GDPR Articles 7 & 21)". The provider is therefore referring to a different legal basis for processing. Article 7 regulates the conditions for obtaining valid consent, which refers to the legal basis under Art. 6(1)(a) GDPR, whereas Article 21 outlines the right to object discussed at this point, which may be exercised where processing is based under Art. 6(1)(e) or (f). It is therefore not clear what kind of request a "Do-Not-Track" signal would in fact support.

The reason for this quite vague wording lies in a general problem with legally justifying such requests. This stems from a conflict between the General Data Protection Regulation and Directive 2002/58/EC, also referred to as the E-Privacy Directive. Originally Article 5(3), which concerns confidentiality of communication and provided rules for storing information or gaining access to such saved on the terminal equipment of a user or subscriber, stated that this should be allowed where the individual concerned *"is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC"*.[1053] This wording was, however, amended in 2009 and now includes a requirement for the person in question to have given *"his or her consent"*.[1054] While this does not apply to processing strictly necessary for the provision of services requested by the data subject, this exemption only covers elements such as cookies needed for allowing the functioning of an online shopping cart or

---

[1053]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[1054]Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

a chatbot, and typically does not include any tracking performed for marketing purposes.[1055]

The requirement for "consent" contained within Art. 5(3) of the E-Privacy Directive therefore sparked a heated debate with regards to the relationship between this provision and the GDPR, including the question whether or not this meant that GDPR compliant consent was necessary for the deployment of cookies and other tracking techniques.[1056] The conflict did not gain much relevance in certain jurisdictions such as the Netherlands, Austria or Portugal, which enacted laws transposing the E-Privacy Directive that explicitly required the user's consent.[1057] In Germany, however, where the Telecommunication and Telemedia Law (TTDSG)[1058] only came into force in December 2021, the question was a cause for much uncertainty for over a decade.[1059] Since the CJEU's decision on *Planet 49*,[1060] the

---

[1055] *Piltz/Kühner*, 3 ZD 2021, 123, 126f; *DPC*, Guidance on Cookies, 6f; *Art. 29 WP*, Opinion 04/2012, 6.

[1056] *Haberer*, MMR 2020, 810, 811f; *Rauer/Ettig*, 6 ZD 2015, 255, 257f; *Schmidt/Babilon*, 2 K&R 2016, 86, 86-90; Hoeren/Sieber/Holznagel / *Schmitz*, 'Teil 16.2 Datenschutz im Internet' in Thomas Hoeren, Ulrich Sieber and Bernd Holznagel, HdB MultimediaR, Teil 16.2, para 274-277.

[1057] *Rauer/Ettig*, 6 ZD 2015, 255, 258.

[1058] In May 2024 the TTDSG was replaced by the Telecommunications Digital Services Data Protection Act (TDDDG). The changes were, however, minimal and predominantly relate to adaptions in order to reflect the terminology of the Digital Services Act correctly. See: Bundesgesetzblatt, , Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze', https://www.recht.bund.de/bgbl/1/2024/149/VO (accessed 24 October 2025).

[1059] *Rauer/Ettig*, 1 ZD 2014, 27, 27 ff; *Rauer/Ettig*, 6 ZD 2015, 255, 255-259; *Rauer/Ettig*, 9 ZD 2016, 423, 423ff; *Schmidt/Babilon*, 2 K&R 2016, 86, 86-90.

[1060] Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 65.

subsequent "*Cookie-Consent-II-Ruling*" of the Federal Court of Justice[1061] and the now applicable § 25 of the TDDDG[1062] which explicitly requires GDPR-compliant consent for storing information or gaining access to such saved on the terminal equipment of an end-user, the debate does seem at last to have come to an end.[1063]

While the final resolution of this long-lasting debate is to be considered an important step, it also has significant consequences for the legal status of Do-Not-Track-Techniques, namely that Art. 21 cannot be used as a legal justification for such. After all, if the sole legal basis which can be used for the implementation of such tracking techniques is consent under Art. 6(1)(a), then objection, which applies for processing activities based on Art. 6(1)(e) or (f), will in fact never apply. This is also not changed by any means through the exemption introduced for processing which is "strictly necessary" for the provision of information society services explicitly requested by the individual, since the legal basis for such would in principle be Art. 6(1)(b). On the other hand, considering a direct request of a browser, the withdrawal of consent under Art. 7(3) is logically inconsistent as the user would have to have given consent in the first place. Since their legal status is largely unclear or rather unsupported,[1064] it seems that at least for EU-based jurisdictions, Do-Not-Track tools have, as of late 2024, missed their moment to truly become relevant. In this context, the offering of a functionality by Personal Information Management Systems, which would allow individuals to effectively enforce their right to objection in the context of online tracking, is largely pointless.

[1061]BGH, NJW 2020, 2540.

[1062]*Hanloser*, 3 ZD 2021, 121, 121.

[1063]*Rauer/Ettig*, 1 ZD 2021, 18, 18ff; *Spindler*, 35 NJW 2020, 2513, 2513 ff; *Böhm/Halim*, 10 MMR 2020, 651, 654.

[1064]Such an assessment is currently supported by the ICO, which stated with regard to the Global Privacy Controls that: *"the GPC does not at this time appear to offer a means by which user preferences can be expressed in a way that fully aligns with UK data protection requirements.*". See: https://ico.org.uk/media2/tss-jamaw/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf (accessed: 04 March 2026).

(b) Other Alternatives

While the ability to effectively block the tracking of user behaviour for marketing purposes would have been an interesting functionality, alternative possibilities of enforcing this right can still be explored. The current tendencies in the legal classification of such tracking methods make them largely irrelevant in the context of the right to object under Art. 21. As mentioned before, since data subjects are not required to provide any explanation for their objections in the context of direct marketing, both automated and generalised multi-controller submissions of objections are still possible. To that extent, Personal Information Management Systems, which have specialised themselves in mass submissions of deletion requests, will *often* also rely on that legal basis.[1065] While the legal validity of such "mass requests", which sometimes simply mention any type of legal basis available globally,[1066] is also to an extent questionable, they do effectively force controllers into dealing with the matter in some capacity. The outcome is most likely varied but in more or less uncritical instances where the individual's data is part of a marketing or newsletter database, it can be assumed that businesses would still remove the individual from such, based on these requests. While, therefore, certainly not the most elegant and sophisticated solution neither from a technical nor legal perspective, a certain efficiency of these cannot be denied.

[1065]For example: Mine, http://saymine.com/ (accessed 22 February 2026); Privacy Bee, http://privacybee.com/ (accessed 22 February 2026); DeleteMe, http://joindeleteme.com/ (accessed 22 February 2026); Revoke, http://revoke.com/ (accessed 22 February 2026); My Data Done Right, https://www.mydatadoneright.eu/faq (accessed 22 February 2026).

[1066]For example requests submitted by Privacy Bee contain the following extremely broad wording: "*I am hereby submitting a follow-up to a personal data request pursuant to Section 1798.105 of CCPA (SB-1121), Article 17 of GDPR, Nevada SB-220, New Hampshire HB 1680-FN, Washington Privacy SB-5376, Illinois DTPA SB2330, New York S5462, Hawaii SB 418, North Dakota HB 1485, Massachusetts S-120, Maryland SB 613, Texas Privacy Protection Act HB 4390, or other applicable right-to-be-forgotten legislation.".* See: https://iapp.org/news/a/why-some-dsr-services-create-compliance-concerns/ (accessed: 22 February 2026).

bb) Consequences

In accordance with Art. 21(1), the controller should no longer process the personal data in question in cases where a successful request for objection has been made. Businesses will therefore in principle be obliged to deletion or anonymisation of such data, as any form of further retention or use would still constitute processing in the meaning of Art. 4 No. 2.[1067] This is also supported by Article 17(1)(c), which stipulates that the data subject has the right to obtain erasure from the controller where that person has objected to the processing and no overriding legitimate grounds have been identified. While the verification of these grounds is still pending, the dataset may be subject to restriction in accordance with Art. 18(1)(d). The same would also apply where the individual explicitly requests its restriction, instead of erasure (Art. 18(1)(b)).[1068] Another instance in which immediate deletion might not be warranted and, in fact, to a certain extent be against the interests of the data subject, concerns objections in the context of direct marketing. As outlined under Part 1 Chapter 2: D. II. 6. a) cc) Direct Marketing, the maintenance of so called "blacklists" or "suppression lists" of individuals who do not wish to be further contacted is from a practical standpoint necessary in most instances.[1069] While legally such an operation constitutes a new processing activity for a different purpose (assuring that the individual's wishes are complied with), it can in a sense also be considered a form of "restriction".

Since the practical consequence of the right to objection will either lie in the deletion or restriction of the processing of a certain dataset, the PIMS functionalities relating to such will also largely correspond to those two modalities. As potential features supporting the right to erasure and the right to restriction have already been analysed under Part 1 Chapter 2: D. II. 3. c) Technical Execution, Challenges and

---

[1067]Paal/Pauly / *Martini*, Art. 21 DSGVO, para 46; Kühling/Buchner / *Herbst*, Art. 21, para 25; Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 23.

[1068]Paal/Pauly / *Martini*, Art. 21 DSGVO, para 45.

[1069]Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 23; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 26; Kühling/Buchner / *Herbst*, Art. 21, para 32a.

Potential for Advancements and D. II. 4. c) Involvement of PIMS, their entire reiteration would at this point be superfluous. As a reminder, it is, however, worth mentioning that there are in fact a number of technical and organisational obstacles connected to the assurance of comprehensive deletion of an individual's data across all data stores of a business. In that context, the deployment of automated expiration dates for certain datasets and the facilitation of retrospective data revocation are to be considered potential features, in the context of enabling the right to objection as well. The same also applies for so called "Data Revocation Services", which allow the creation of push and pull notices to controllers, based on the use of unique data identifiers.

In the context of restriction, the proposed functionality of having the data stored by the Personal Information Management System, while a resolution of a conflict between the data subject and the controller is still pending, applies to the verification of the existence of overriding legitimate grounds as well. As a consequence, the data subject would be reassured that no illegitimate activities are taking place, while controllers would no longer be burdened with separating and securing the information. Also, while the maintenance of a suppression list for purposes of direct marketing by a third party might at first seem counter-intuitive as the controller would require constant access in order to assure that the wishes of the individual are complied with, it is in fact not only imaginable, but already practised to a certain extent in other areas. After all, the National Do Not Call Registry maintained by the FTC in a sense constitutes exactly that: a list of individuals who do not wish to receive telemarketing calls, kept in a centralised manner for all concerned businesses to access.[1070] Therefore, the implementation of an equivalently centralised solution by a trusted provider of Personal Information Management Systems, would at least theoretically be possible.

[1070]FTC National Do Not Call Registry, https://www.donotcall.gov/ (accessed 24 October 2025).

d) Interim Conclusions: Objection

on the legitimate interest of the controller (Art. 6(1)(f) GDPR) or on the necessity for the performance of a task carried out in the public interest or in the exercising of official authority vested in such (Art. 6(1)(e) GDPR). In principle, an objection has to be based on grounds relating to the particular situation of that individual, with an exemption applying in the context of processing for the purposes of direct marketing. Controllers are also allowed to continue the processing of personal data where they can assert the existence of compelling legitimate grounds which override the interests of the individual. There are no explicit requirements as to the format in which such requests should be submitted. A written format is, however, generally advised for documentation purposes. Also, all objections except those provided in the context of direct marketing, will require some sort of justification from the individual. Where the processing of personal data relates to the use of information society services, controllers are additionally obliged to facilitate the exercise of the right to objection, although by automated means and using technical specifications in accordance with Art. 21(5).

Since the typical management of a submitted objection will require an analysis of the individual's particular situation as well as the consideration of any overriding interests or legal claims which might occur, the room for the involvement of a Personal Information Management System at that level is quite limited. It is, however, imaginable in the context of submitting a request or when implementing its consequences. The submission of an objection through PIMS could, for example, be constructed more conveniently for individuals through the features such as standardised identification procedures or the automatic calculation of deadlines. Also, since objections to processing for direct marketing purposes do not require the individual to provide any reasoning, more or less automated and generalised submissions to multiple controllers at once could be facilitated. In that context, the deployment of so called "Do-Not-Track" technologies, which allow for users to automatically opt-out of any tracking performed by websites they visit, has been considered for a long time.

At least on the European market these techniques, however, seem to have missed their moment for gaining relevance, as Article 5(3) of the E-Privacy Directive effectively requires the provision of consent for all types of online tracking techniques which are not strictly necessary for the provision of a service requested by the data subject. In that context, Art. 6(1)(e) and (f) are virtually excluded from being considered a legal basis for such processing operations, making the right to object in that context insignificant. Independently from the stipulations in the context of cookies and other methods of collecting user data, automated submissions of requests through a PIMS can still be considered. There are, in fact, a number of service providers offering such a management of "mass requests", with the promise of removing the individual's information from all types of databases which also at times use the right to object as their legal basis.

Personal Information Management Systems can also, to a certain extent, be considered as supporting the right to objection where they facilitate the implementation of its consequences. Since such will either constitute the erasure of the datasets in question or the restriction of their processing, the functionalities analysed in that context will apply correspondingly. Particularly worthy of mention are data revocation services, allowing the data subject the de-identification of one's information either directly or through the use of push or pull notices. Regarding the restriction of processing, the storage of any personal data directly with the PIMS provider for the time in which the verification of the existence of overriding legitimate grounds is still pending could bring multiple benefits both on the side of the data subject and the controller. Finally, the implementation of a centralised databank of individuals opting out of direct marketing in certain contexts or even in general, managed in a similar manner as the National Do Not Call Registry maintained by the FTC, could be considered.

III. Interim Conclusions: Request

The above section has focused on the possibilities in which Personal Information Management Systems could support data subjects

in the exercise of their rights of access, rectification, erasure, restriction, portability, and objection. Since the enforcement of these rights will generally require an action in the form of a request directed towards the controller to be taken by the individual, they would presumably be particularly relevant in the context of PIMS. The above analysis does not, however, seem to entirely support this presumption.

The most developed service offerings in that regard can be observed in the context of supporting the right to data portability. Here, both solutions directly endorsed by data controllers such as the Data Transfer Project, as well as such offered by third party intermediaries such as MyDex, World Data Exchange, CozyCloud, or Citizen.me, can be found on the market. While they are to a large extent capable of allowing individuals to control their data transfers and facilitate a better understanding of the occurring data flows, there are still some limitations in ensuring full data portability which are predominantly the result of inconsistencies in formats and lack of interoperability between different platforms.

There are also a number of tools offering the more or less automated submission of requests for deletion or objection to the processing on behalf of the individual. The services provided by these types of PIMS do not, however, typically go beyond simply submitting a request and informing the data subject of its outcome, without actually assuring the compliance of the controller with such. More advanced technical solutions for the effective enforcement of these rights are, however, being developed outside of the realms of “typical” PIMS. These include approaches such as the creation of expiration dates for data sets or allowing data revocation through the use of unique identifiers and the introduction of push and pull notices.

The support of access requests is also largely limited to a type of automated “mass submission”, as mentioned previously. Even lesser service offerings from Personal Information Management Systems can be identified in the context of assuring the rights rectification and restriction of processing, which does not seem to be within the focus of these tools at all. This lack of offered solutions is therefore quite

surprising, taking into account the previously determined and presumed suitability of these rights for the inclusion in PIMS.

Based on this, the section has also largely explored potential functionalities which could in fact be integrated into PIMS in order to support these rights, taking into account the state of technical developments. It is concluded that already existing solutions for machine learning and natural language processing, presented in the context of transparency enhancing technologies, could be used for the provisions of a type of automated quality control or in order to review the accuracy of statements made by the controller. Also, analogous to the already established practices of data repositories in the field of scientific research, the PIMS could secure the data in question for the purposes of restriction on behalf of the controller. Furthermore, less technical based solutions, such as the simple assurance of request specifications, secure identification procedures, deadline calculation, or the provision of check-lists to the controller have been suggested, allowing a more effective exercise of the individual's rights.

E. Findings for Part 1

A uniform definition for the term "Personal Information Management Systems" does not exist at the moment. The most broadly accepted version, with some variations, does, however, seem to be the one established by the European Data Protection Supervisor, which describes them as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*. This is also the definition which has been applied for the purpose of this thesis, with other types of PIMS such as compliance tools, organisers, or HR-systems explicitly excluded from the scope. Part 1 of this thesis serves the purpose of establishing the existing as well as potential functionalities offered by PIMS, in order to allow the subsequent analysis of the possible role they will take towards the data subject under the GDPR.

It can be concluded that the focus of service providers in this context has been put on the functionalities relating to secure data storage and consent management. The comparatively large amount of secure storage solutions can easily be equated to the fact that these are arguably most easily deployed, considering the current state of technical developments. Also, the storage of data, whether with the PIMS or on the user's device, will inevitably be necessary in the context of any type of service offering, making it a sort of universe functionality for all PIMS. The considerable amount of consent management tools, on the other hand, is likely based on the extensive criticism directed towards the current forms of obtaining consent, particularly in the online environment. The analysis of the offered solutions has demonstrated, however, that while some of the commonly known problems could to a certain extent be mitigated, the currently available consent management platforms are still subject to many limitations and are unable to solve all of the identified problems. On the other hand, the reviewed types of transparency enhancing technologies supporting individuals in gaining a better understanding of the controller's processing operations which serve the purpose of supporting the data subject right to information, are quite promising and effective.

Whereas the functionalities of "storage", "information", and "consent", analysed in Sections A, B and C of Chapter 2, included many practical examples of platforms offering such services, the same could not be achieved in Section D, which focused on the support of PIMS in enforcing data subject requests. The only right which seemed to be prominently offered by actual PIMS was the one of data portability, with all others either being surprisingly underdeveloped (access, erasure, and objection) or, even more so, completely ignored (restriction and rectification). The reasons for the lack of focus in these rights are not clear, especially considering the various forms in which their enforcement could in fact be advanced by already technically feasible solutions. It could, however, be speculated, that providers might see a larger potential in the first three types of offerings since they relate to obligations with which controllers are required to comply per default, whereas those analysed in

Section D only demand action in the case a request is made by the data subject. Since currently the platforms most advanced from a business perspective still largely depend on a cooperation with the controller, it makes sense that these would focus on functionalities which are of the most interest to those.

Taking into account overall market realities, it can safely be concluded that the idea of Personal Information Management Systems supporting data subjects in effectively enforcing their rights and taking more control over their personal data has definitely gained significance over the last decade and is still consistently being furthered. This means that questions regarding the legal standing of PIMS, their relationship with the individual, and the resulting obligations as well as liabilities should certainly be clarified.

Part 2

The Old Predicaments Strike Back

Roles taken by Personal Information Management Systems under the GDPR

Part 2 of this thesis was focused on explaining the term “Personal Information Management Systems”, in particular the definition taken as a basis for this analysis and examining the potential of these systems to support the individual in the exercise of their rights under the General Data Protection Regulation (GDPR). In comparison, Part 2 will focus on the main question of this thesis which is the division of the roles and responsibilities among the parties involved in the processing of personal data in the context of PIMS. For that purpose, the different functions foreseen by the GDPR, namely those of the controller, processor, joint controller, third parties and recipients, will first be defined in Chapter 3. Taking those definitions as a basis, the functionalities of Personal Information Management Systems, presented in Part 1, will be analysed with regards to the roles taken by those tools under the GDPR. This analysis will be performed in Chapter 4.

Chapter 3

Roles defined in the GDPR

Correctly assigning the different roles of controller, processor, joint controller or third party, as defined by the GDPR, to the various actors involved in the processing activity is not only a purely academic exercise but carries important practical implications with regard to the responsibilities, accountability, and liabilities of the parties. It will also directly affect how, where, and to what extent the data subject will be able to exercise their rights, which makes it crucial to clearly define these roles in advance and therefore avoid any legal uncertainties. However, while the concepts themselves seem pretty simple at first glance, increasingly complicated corporate structures and the rising trend towards the outsourcing of non-core business activities often make it difficult to accurately assign the roles and responsibilities.[1] What adds to the complication is the fact that the GDPR does not recognise an intra-group privilege, meaning that where tasks are being performed by different legal entities under the same corporate umbrella, the relationship between these will still need to be examined and contractually established.[2] Also, since these are functional concepts, they need to be interpreted according to the actual activities taken by the parties in a specific situation, meaning that the actors are not free to simply agree on a certain designation and thereby distribution of responsibilities by themselves.[3]

Before beginning the legal analysis, it is important to note that all of these concepts should generally be interpreted autonomously,

---

[1] Rücker/Kugler, *Rücker*, B. Scope of application, para 110.

[2] *Voigt/von dem Bussche*, GDPR, 18.

[3] *Bassini*, BLP 2019, 103, 108; *EDPB*, Guidelines 07/2020, para 12; *Art. 29 WP*, Opinion 1/2010, 9.

without taking into account other fields of law or national peculiarities.[4] This is important since the differences in national interpretations of these concepts were one of the issues identified by the European Commission in their 2012 Impact Assessment in which the implementation of the Data Protection Directive was evaluated.[5] The Commission pointed out that the legal uncertainty caused by different national interpretations is not only hindering the free flow of personal data within the internal market by creating additional cost and administrative burdens for stakeholders but also negatively affects the data subjects as it potentially distorts the equivalent level of protection which should have been ensured under the Directive.[6] Still, other laws may have an effect on the roles taken by the parties under the GDPR, where they either explicitly or implicitly assign responsibility to an entity which naturally correlates with controllership over a processing activity (see Part 2 Chapter 3: A. II. 1. a) Legal Designation). The notion of interpreting provisions of community law *"in the light of the provisions of community law as a whole"* has also expressly been supported by CJEU case law in the past.[7] Especially in consumer protection law, the idea of viewing the different legal acts as part of a single, comprehensive set of rules which complement each other, has been supported.[8] The impact of certain terms and legal concepts in Union Law on other areas has also further been supported in the Judgements of *Bankia* and *Pereničová and Perenič.* [9] While the subsequent section will

---

[4] *EDPB*, Guidelines 07/2020, para 14.

[5] *European Commission*, Commission Staff Working Paper Impact Assessment (25 January 2012) Annex 2, 17.

[6] ibid.

[7] Case 283/81 CILFIT and Lanificio di Gavardo [1982] ECLI:EU:C:1982:335 para 20.

[8] Case C-453/10 *Pereničová and Perenič* [2012] ECLI:EU:C:2012:144, Opinion of the AG Trstenjak, para 88.

[9] Case C-109/17 *Bankia* [2018] ECLI:EU:C:2018:201, para 49; Case C-453/10 *Pereničová and Perenič* [2012] ECLI:EU:C:2012:144, para 43f. For a more detailed analysis refer to: *Hacker*, Datenprivatrecht, 335-339, also: *Keirsbilck*, 50 Common Mark. Law Rev. 2013, 247, 258.

therefore focus strictly on the division of roles found in the GDPR, Part 3 of this thesis will also incorporate considerations of other legal acts and analyse how those might potentially affect the roles taken by the parties (See Part 3 Chapter 6: Liability outside the GDPR).

A. Controller

According to Art. 4 No. 7 GDPR, “controller” refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It also clarifies that where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

I. Personal Element

The GDPR does not put any restrictions on the type of entity that can be considered a controller, clearly stating that it can be any “natural or legal person, public authority, agency or other body”. This means that the legal form of the controller is not relevant for the determination of the responsible body.[10]

1. Legal Person

While the GDPR does allow for the possibility of a natural person being a data controller, those instances are rare in practice, since processing of personal data in the context of someone’s private life will likely be covered by the household exemption under Art.

---

[10] *Voigt/von dem Bussche*, GDPR, 18; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 9; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, 'Art. 4 Nr. 7 DSGVO, para 16; Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 55.

2(2)(d).[11] If, on the other hand, an individual is acting within an organisation, the organisation will in most cases remain the controller, even if there is significant decision-making power behind the individual (such as the CEO or management board).[12] This preference for considering the company as the data controller has multiple reasons. It is supposed to ensure a clear and unequivocal identification of the controller, while also providing the data subject with a stable and reliable reference entity for the exercise of their rights.[13] Additionally, it should be noted that executing fines from a legal entity will, in most instances, be more efficient and effective than doing so from a natural person.

Questions can, however, arise as to where the responsibility lies in complex organisation structures such as larger groups of undertakings.[14] Recital 37 introduces in this context a differentiation between "controlled" and "controlling" undertakings, remarking that the "controlling" should be done by the ones executing *"a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented"*. Based on that, some sources have put forward the suggestion that in the case of doubt, the dominating company holding the principal resources, as well as central management, should be considered the controller.[15] While this approach may be taken, where the localisation of responsibility is otherwise completely impossible the primary focus should, however, always be on the actual source of

---

[11] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, 'Art. 4 Nr. 7 DSGVO, para 14.

[12] *Monreal*, 12 ZD 2014, 611, 612; *EDPB*, Guidelines 07/2020, para 17; *Voigt/von dem Bussche*, GDPR, 18; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 149.

[13] *Art. 29 WP*, Opinion 1/2010, 15; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 9.

[14] Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 9.

[15] Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 41; Sydow/Marsch / *Raschauer*, Art. 4, para 133.

authority when it comes to the processing activity, not overall business decisions.[16]

It should be noted in that context that while determining the legal entity which will be held responsible for a particular processing activity towards the data subject, it has generally been established that the impression given to the data subject should also be taken into account.[17] While this is by no means to be considered a decisive factor, it has in the past been used as a consideration in determining the respective roles of the parties.[18] Where therefore a certain business is directly collecting data from a person or communicating with such, even though they may technically be doing so on behalf of someone else, they could be construed as a separate or joint controller where they have failed to communicate the identity of the actual controller transparently, in accordance with the requirements of Art. 13 and 15 of the GDPR.

2. Natural Person

Whereas the consideration of natural persons as data controllers is certainly less common, there are instances where this might still occur.

a) Conventional Examples

Typically this will, for example, be the case in the context of certain freelance and liberal professions, where individuals are acting as sole traders or their specific occupation is subject to requirements of professional secrecy, making oversight over their processing activities illegal.[19] This is due to the fact that these professions

---

[16]Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 42.

[17]Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 149; *Lindqvist*, 26 Int. J. Law Inf. Technol. 2018, 45, 49.

[18]See for example: Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551, para 21: „*the conception that the data subject has of the controller must be taken into account*".

[19]*Petri* / Simitis/Hornung/Spiecker gen. Döhmann, 'Art. 4 Nr. 7 DSGVO, para 14.

require the individual to have full control and authority over the entire operation, including the processing of personal data and not to be bound by instructions from other parties.

As outlined before, the actions of employees are, however, generally still considered as falling under the responsibility of their employer, who will be considered as the "controller" for all processing activities performed in the context of the employment relationship.[20] This rule will not apply, however, where the individual acting within a legal entity *"uses data for his or her own purposes, distinct from those of his or her employer"*.[21] Such "rogue employees" will then be considered controllers in their own right and consequently also bear the administrative and criminal liability for their actions.[22]

A natural person might also inadvertently turn out to be the data controller as a result of the narrow interpretation of the household exemption. This is mostly the case in which an individual wrongly believes that his or her processing activities are occurring solely in the course of a purely personal or household activity. Examples include cases such as *Bodil Lindqvist,*[23] *František Ryneš,*[24] and

---

[20]Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 9.

[21]*EDPB*, Guidelines 07/2020, para 86.

[22]*EDPB*, Guidelines 07/2020, para 86; *Ambrock*, 10 ZD 2020, 492, 495ff; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 10.

[23]Case C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596, para 47. A Swedish catechist had set up a website in order to help parishioners preparing for confirmation. The website also contained information about personal details (including sensitive personal data) of her and her colleagues. The ECJ ruled that processing of personal data *'consisting in publication on the internet'*, which is being *'made accessible to an indefinite number of people'* can clearly not be considered as being carried out in the course of private or family life (para 47).

[24]Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428. Mr. Rynes, whose family and property had for several years been subject to multiple attacks, had installed a camera, which recorded the entrance to his home, the public footpath and the entrance to the opposite house. The ECJ ruled that where the video surveillance, even partially, covers public spaces it cannot be considered a purely personal or household activity (para 33).

Jehovan todistajat,[25] which have all been submitted for preliminary ruling to the European Court of Justice.

b) Data Subjects

Directly related to the household exemption is another crucial question which has increased in relevance over the years and is subject to much debate, namely whether or not a data subject could be regarded as a controller under the GDPR.[26] The thought process behind this idea is that essentially it is the data subject that most frequently decides on how their information is being processed by providing consent, sharing it with third parties, entering it in forms or web-pages, or securing it at home in folders or on their hard drives. In that sense, it could be considered that the data subject is determining the means and the purposes of the processing of their personal data.[27] After all, the European Data Protection Board has in fact confirmed that *"in principle, there is no limitation as to the type of entity that may assume the role of a controller"*.[28] On the other hand, however, the GDPR does seem to introduce a clear division of the involved actors into controllers, processors, and data subjects,

---

[25]Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551. The case concerned the collection and processing of personal data by the Jehovah's Witnesses Community in the course of their door-to-door preaching activity. In its judgement the ECJ confirmed that such a practice does not fall under the household exemption, since the activity is "is directed outwards from the private setting of the members who engage in preaching" (para 44). Also, the lists of people who no longer wished to receive visits were sent to the congregations, which means that part of the data collected was being shared with a potentially unlimited number of people (para 45).

[26]*Wagner*, 7 ZD 2018, 307, 307; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Finck*, Blockchain Regulation, 101; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212; *Finck*, 11 IDPL 2021, 333, 338.

[27]Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154.

[28]*EDPB*, Guidelines 07/2020, para 17.

making it impossible for one party to be considered as both with regards to a specific processing activity.[29]

The questions were arguably not as relevant in the past, since naturally most processing of personal data concerning oneself would be considered a purely personal activity and thereby fall outside of the Regulation based on the household exemption under Art. 3(2)(c). Technological developments such as smart-homes, social media, or blockchain have, however, lead to the fact that seemingly "personal" activities are being increasingly externalised and transpired to the outside world.[30] This fact is accompanied by two interpretational tendencies of the Court of Justice of the European Union (CJEU). First of all, the CJEU established a narrow interpretation of the scope of *"purely personal or household activity"* in the cases of *Bodil Lindqvist* and *František Ryneš,* clearly excluding any type of activities directed outside of the private setting of one's own home, either by way of collection or publication.[31] At the same time, a quite broad interpretation of the definition of controller was ascertained in the cases of *Wirtschaftsakademie Schleswig-Holstein*,[32] *Jehovan todistajat,*[33] and *Fashion ID,*[34] essentially including anyone who contributes to the processing or makes it possible into the scope.[35] The combination of these factors has therefore potentially caused a

---

[29]Sydow/Marsch / *Raschauer*, Art. 4, para 119; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154.

[30]*Chen and others*, 10 IDPL 2020, 279, 289; *Finck*, 11 IDPL 2021, 333, 339f; *Wagner*, 7 ZD 2018, 307, 311.

[31] See: Case C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596, para 47 and Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, para 33.

[32]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388.

[33]Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551.

[34]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.

[35]For more details on the developmental tendencies of broadening the term refer to Part 2 Chapter 3: C. III. Case Law of the Court of Justice of the European Union, below.

shift in responsibility towards individual users.[36] Since the GDPR does explicitly include natural persons into the scope of potential controllers, it does make sense to make them responsible where they make crucial decisions regarding the processing of the personal data of other individuals. This is seen in examples such as publishing tagged pictures on social media, inviting guests into a smart home, or giving someone a ride in a connected car. In such instances, the natural person would likely be considered a joint controller together with the service provider.[37]

The assumption of the position of controller with regards to one's own personal data does, however, seems problematic. In that context, the aim of the General Data Protection Regulation should be taken into account. Both Article 1(1) and Recital 10 point to the protection of natural persons as the objective of the Regulation. If data subjects were now subject to the responsibilities set out for controllers, this would in effect burden them, rather than assure their protection.[38] Also, while data protection law places significant weight on the idea of informational self-determination, it does not support the idea that this is absolute as the GDPR does clearly include rights and protections which need to be assured by controllers and cannot be waived by the individual.[39] If an individual was to be considered a (joint) controller for their own personal data, they could be potentially deprived of the possibility of exercising certain rights against other entities, if it were to be assumed that the assurance of those falls under their obligation.[40] Such an outcome can most certainly not be considered as in the interest of assuring "*effective and complete*" protection, established by the CJEU case law.[41] In light of these

---

[36]*Edwards and others*, IPR 2019; *Wagner*, 7 ZD 2018, 307, 311; *Finck*, 11 IDPL 2021, 333, 338f.

[37]*Wagner*, 7 ZD 2018, 307, 312; *Edwards and others*, IPR 2019.

[38]Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154.

[39]*Finck*, 11 IDPL 2021, 333, 343.

[40]*Edwards and others*, IPR 2019.

[41]Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154.

issues, the assumption of controllership by the data subject themselves should not be supported.[42]

II. Substantive Element

While the personal element of the definition opens it up to anyone, it is here where the real meaning of the term is defined. The data controller will be the party which "*determines the purposes and means of processing personal data*".

1. Determination

Determination means "*the process of deciding something officially*".[43] Therefore, in order to be considered a controller, the party needs to have decision-making power with regards to the processing activity.[44] In that sense, it is largely irrelevant what entity is in fact physically conducting the processing activity, as the question of authority over the process will be considered the decisive element.[45] Such power could either stem from a legal obligation to perform a certain processing activity or from the factual circumstances of a certain case.

a) Legal Designation

The legal designation as a controller could either result from an explicit or an implicit legal responsibility.

---

[42]Sydow/Marsch / *Raschauer*, Art. 4, para 119; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212.

[43]Oxford Learners Dictionaries, https://www.oxfordlearnersdictionaries.com/definition/academic/determination (accessed: 24 October 2025).

[44]*EDPB*, Guidelines 07/2020, para 19; *Voigt/von dem Bussche*, GDPR, 19; Sydow/Marsch / *Raschauer*, Art. 4, para 123.

[45]; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, 'Art. 4 Nr. 7 DSGVO, para 20; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 37.

aa) Explicit Legal Responsibility

Explicit legal responsibility is mentioned in Art. 4(7) GDPR which states that *"where the purposes and means of such processing are determined by Union or Member State law, the controller of the specific criteria for its nomination may be provided by Union or Member State law"*. This means that the law will explicitly set out who the controller should be or what the criteria for its nomination are. Examples of such an explicit designation can be found in the Irish Data Protection Act 2018. According to Section 3(1), public authorities may designate an individual civil servant to be the data controller and Section 3(2) provides that the Minister for Defence may designate an officer of the Permanent Defence Force, holding commissioned rank, to be controller. These kind of explicit designations, however, are still rare.

bb) Implicit Legal Responsibility

What is more common are implicit legal designations in which the legal provision establishes a task or a responsibility which cannot be fulfilled without processing personal data.[46] In those instances, while the natural or legal person upon which the task has been imposed might not have any interest or desire in executing the task in question or processing any personal data in this context, they will still be considered a controller since the processing is necessary for the execution of their legal obligations. This also typically includes legal requirements to disclose or transfer personal information to other (typically public) entities, such as law enforcement or tax authorities. Examples of such implicit legal designations can basically be found

---

[46] *EDPB*, Guidelines 07/2020, para 22; *Voigt/von dem Bussche*, GDPR, 19; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 14.

in all areas of law but are most commonly seen in areas such as social security,[47] tax,[48] or labour law.[49]

Even legal norms which do not contain any specific obligation to process personal data but regulate the relationship between two parties, can also help indicate a certain responsibility towards the data subject and therefore help with the identification of the data controller. This will in particular be the case when it comes to certain professions which by themselves require a level of authority or trust from the other party. Such professions would include lawyers, accountants, publishers, or associations which process the personal data of their members and contributors, as their role as a controller would be "naturally attached" to their position.[50] Implicit legal obligations might also result from the relationship between a certain entity and the data subject, especially where traditionally the roles taken by those parties imply specific responsibilities.[51] This is for example typically recognised in the relationship between an employer and an employee.[52]

b) Factual Influence

While influence can stem from legal obligations or established legal practices, this will not always be the case. Where control cannot be derived from other sources, the factual circumstances of the processing need to be analysed.[53] The determination of the controller will be straightforward where only one party is involved in

---

[47]Collecting information about the financial status of applicants for social welfare.

[48]Processing information about employee's family status or religious affiliation for payroll processing.

[49]Legal requirements for first-aid trainings for employees, mean that the employer will need to keep participation lists in order to demonstrate compliance.

[50]*EDPB*, Guidelines 07/2020, para 25; *Art. 29 WP*, Opinion 1/2010, 10.

[51]*EDPB*, Guidelines 07/2020, para 25; *Radtke*, Gemeinsame Verantwortlichkeit, 112.

[52]ibid.

[53]*EDPB*, Guidelines 07/2020, para 23; *Art. 29 WP*, Opinion 1/2010, 11.

the processing of personal data. However, as already mentioned above, in today's interconnected economy this is rarely the case anymore. As soon as multiple players take a role in the processing activity, their respective influence needs to be examined closely.[54] While assessing the contractual terms between the parties can often be helpful in determining the respective roles they take with regards to the processing activity, one needs to remember that since these are functional concepts, they need to be interpreted according to the actual activities taken by the parties in a specific situation, regardless of their contractual designation.[55] This means that it is not sufficient to define a party as the "controller", the entity needs to have actual substantial influence over the processing activity and thereby act on its decision-making power.[56]

2. Means and Purpose

This second part of the substantive element of the controller definition links directly to the element of determination, as it shows us over what it is that the data controller should exercise their decision-making power. This is also commonly referred to as the "why" and "how" of data processing, meaning the controller should determine why personal data is being processed in the first place and how this should be done.[57] This again is a very straight-forward exercise where only one party is involved in the processing of personal data but which becomes increasingly difficult as other actors, who take over certain tasks and responsibilities with regard to the processing, get involved.

When assessing who is responsible for the determination of the means and purposes of processing in multi-party constellations, the

---

[54] *Bassini*, BLP 2019, 103, 110.

[55] *EDPB*, Guidelines 07/2020, para 26f; *Art. 29 WP*, Opinion 1/2010, 11.

[56] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, 'Art. 4 Nr. 7 DSGVO para 20; *Bassini*, BLP 2019, 103, 109.

[57] Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 150; Ustaran / *Macmillan,* Chapter 4, 89; *Voigt/von dem Bussche*, GDPR, 19; *EDPB*, Guidelines 07/2020, para 33.

question arises as to what level of detail a party needs to be making these decisions in order to be considered a controller and to what extent a processor should be granted with a margin of manoeuvre in making their own decisions regarding the processing activity.[58] The general consensus in that area seems to be that the determination of the purpose of processing can only lie on the side of the controller.[59] The means of the processing, however, should be divided into "essential" and "non-essential" means; where decisions about the first are still reserved for the controller, the latter on the other hand are free to be left to the processor.[60] According to this categorisation, essential means would include elements such as the type of personal data being processed, the duration of the processing, and the potential recipients, whereas non-essential means would be limited to questions about the practical implementation such as the specific technical and organisational measures.[61]

3. Processing

The decisions made by the controller need to be concerned with the processing of personal data and not any other elements. While this seems obvious since pursuant to Art. 2(1) GDPR the Regulation only applies to the processing of personal data anyway, it is still important to consider this element, especially in instances where such processing only constitutes a subsidiary effect to the overall

---

[58]Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13; *EDPB*, Guidelines 07/2020, para 35; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 150; *Monreal*, 12 ZD 2014, 611, 612.

[59]Rücker/Kugler, *Rücker*, B. Scope of application, para 134; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13; *EDPB*, Guidelines 07/2020, para 37; *Art. 29 WP*, Opinion 1/2010, 15.

[60]Rücker/Kugler, *Rücker*, B. Scope of application, para 135f; *EDPB*, Guidelines 07/2020, para 38; *Art. 29 WP*, Opinion 1/2010, 14; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 150.

[61]Rücker/Kugler, *Rücker*, B. Scope of application, para 136ff; *EDPB*, Guidelines 07/2020, para 38; *Art. 29 WP*, Opinion 1/2010, 14f.

relationship between the parties, as it is not uncommon for contracting entities to automatically conclude the controllership of the "stronger" counterpart, whether or not this is actually the case. It might, for example, wrongly be assumed that the parent company in a group of undertakings should be considered the controller since this is generally where all strategic decisions will be made. While, however, in many instances this is in fact where the decision-making power regarding the processing activities will lie, this will not always be the case and it is more than common for subsidiaries to be data controllers in their own respect for the processing for certain types of personal data.[62]

Processing, in accordance with Article 4 Nr. 2 GDPR means *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".* It is not difficult to see that this definition is in fact very broad and covers basically any sort of activity (or possibly even complete inactivity in the case of pure storage) relating to personal data. The reason for this can be seen in the legislators' intention to come up with a technologically neutral definition in order to avoid the possibility of circumventing the scope of the application, as has been laid down in Recital 15. Due to that, we are not given any guidance as to what specifically constitutes an "operation", only a non-exclusive list of examples.[63] There is also no differentiation when it comes to the legal consequences of these different types of processing. The same

---

[62]For example, usually each entity will be the data controller with regards to the personal data of their employees. Should certain centralised functions such as payroll-administration, IT-support or running a group directory be provided by the parent or another subsidiary this entity will typically only be a processor.

[63]Rücker/Kugler, *Rücker*, B. Scope of application, para 51; Kühling/Buchner / *Herbst*, Art. 4 Nr. 2, para 20; Sydow/Marsch / *Reimer*, Art. 4, para 53.

requirements apply to all of those regardless of time, place, length or intensity.[64]

a) Set of Operations

The term "processing" may also refer to both a singular operation or to a set of operations, which means that it can either entail one activity or a number of steps which are connected.[65] This might seem slightly derivative as already one action will constitute "processing", making it more or less obvious that multiple such activities will also fall under that term. It does, however, bear significant relevance for multiple reasons. First of all, it again underlines the high level of flexibility that characterises most of the terminology found in the GDPR, showing the express intent that these terms should be adaptable for a multitude of different scenarios. Secondly, it shows an acknowledgement on the side of the lawmaker that while a singular action (such as storing data) will already fall under the scope of application under the Regulation, in practice these will work more as a chain of actions, involving multiple steps from collecting information, reviewing, and structuring it, through to saving and in the end, deleting it altogether. Thirdly, it already implies a certain willingness to possibly "bundle" such activities into one, which is extremely relevant for another crucial term found in the GDPR: "processing activity".

b) Processing Activity

The term "processing activity" is continuously used throughout the GDPR[66] but is never actually defined. From a purely linguistic standpoint, there should be no actual difference between the

---

[64] *Roßnagel* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 2 DSGVO, para 11.

[65] Rücker/Kugler, *Rücker*, B. Scope of application, para 53.

[66] See Articles: 3(2); 4 Nr. 16 b); 24(2); 28(4); 30; 35(6) and (10); 40(6) and (7); 42(6) and 60(10), as well as recitals: 3; 19; 23; 24; 32; 36; 63; 74; 80; 81; 84; 93; 94; 104; 115; 126 and 131.

meaning of "processing" as defined by article 4 No. 2 and "processing activity" as used in other sections, since as discussed earlier, the definition already covers all sorts of activities.[67]

Recital 36, however, draws a clear line between these two terms. This can most evidently be seen in Sentence 4 which states that *"the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment"*. In reading the Recital, it seems as though the term "processing" is used in a more general manner, referring to the overall endeavours of an enterprise, whereas "processing activity" means a concrete undertaking. Sentence 2 for example, mentions *"management activities determining the main decisions as to the purposes and means of processing through stable arrangements"*, relating this to where decisions regarding the processing of personal data are being made in general, not for a specific action. Sentence 5, on the other hand, while talking about the determination of the main establishment, states that where there is no place of central administration in the European Union it should be *"the place where the main processing activities take place in the Union"*, thereby referring to concrete activities, which stand in opposition to other ones, also being performed by the same enterprise.

The same assumption can be drawn when looking at Article 35, in particular Paragraph 10, which stipulates that where processing is necessary for the compliance of a legal obligation or a performance of a task carried out in the public interest, based on the law of a Member State, which also *"regulates the specific processing operation or set of operations in question"* and if a data protection impact assessment had already been carried out as part of the adoption of that legal basis, the requirement to perform an DPIA should no longer apply, unless "*Member States deem it to be necessary to carry out such an assessment prior to processing*

---

[67]Wolff/Brink/v. Ungern-Sternberg / *Spoerr*, Art. 30 DSGVO, para 6; Gola/Heckmann / *Klug*, Art. 30 DSGVO, para 3.

activities". It is therefore evident that, in this instance, the legislator is referring to processing operations while talking about a general type of processing (as these are the operations regulated by Member State law). However, the term "processing activities" is again used when discussing a more specific and individual level, saying that this general exception shall not apply when Member States oblige the controller to carry out such an assessment prior to starting the activity they have planned.

Most importantly, this understanding would also be in line with Article 30, which concerns the so-called "record of processing activities" and should therefore also be considered our main guidance as to the meaning of the term. Article 30(1) requires the controller to maintain a record of all processing activities under its responsibility, which has to contain information regarding the purposes of the processing; the categories of affected data subjects and personal data; the recipients; transfers to third countries; applied security measures; and deletion periods. Analogously, a processor should, according to Article 30(2), keep a record of all categories of processing activities which are carried out on behalf of other controllers. These should include information about the controllers; the categories of processing; transfers to third countries; and, where possible, the applied security measures. The obligation of keeping and maintaining such records is part of the principle of accountability as, according to Recital 82, they are intended to demonstrate compliance with the Regulation and should on request be made available to the supervisory authority for the purpose of monitoring these operations.[68] The processing activities being documented therein will have to refer to specific activities being performed by the controller or processor.[69] This view is also supported by the list of

---

[68] *Laue* / Spindler/Schuster, Art. 30 DS-GVO, para 1; Ehmann/Selmayr / *Bertermann*, Art. 30, para 1; Gola/Heckmann / *Klug*, Art. 30 DSGVO, para 1; Kühling/Buchner / *Hartung*, Art. 30 DSGVO, para 12; Paal/Pauly / *Martini*, Art. 21 DSGVO, para 2.

[69] *Roßnagel* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 30 Nr. 2 DSGVO, para 16 supports a different view, claiming that since the first sentence of Art. 30(2)

information regarding such an activity that needs to be captured, as this will automatically force a certain degree of specification.

This requirement to specify a processing activity should, however, not be taken too far by trying to capture the details of every single sort of operation, as this would lead not only to lengthy and complex but most of all completely incomprehensible and in many respects, redundant records.[70] This is where the definition of processing as an *"operation or set of operations"* and the thereby supported "bundling" of multiple steps becomes relevant. It is generally accepted that multiple "processing" can be condensed into one "activity".[71] This would for example mean that instead of capturing "collecting clients' contact details", "obtaining clients' consent", "entering clients' contact details into database", "saving clients' contact details in database", "using clients' contact details for sending out message" etc. separately, all of these steps would instead be summarised as one processing activity entitled "client database". The same can be said for processing activities which might not be constantly ongoing but reoccurring on a (semi)regular basis (for example, annual events). Here, it would also be redundant to capture the same processing activity every year. Instead, one would summarise this as one

---

talks about the requirement to keep a record of processing activities, whereas point b) only asks for the categories of processing to be included therein; this would suggest that these terms are to be treated as interchangeable. This reasoning however cannot be followed, since the "processing" in b) is part of the description of the "activity" sentence one asks to specify. This specification will only occur in a combination of a), b), c) and d). This means that b) will always have to refer to processing in general (for example "storing") whereas the record will include other specification amounting to a processing activity (for example: "storing data in a data centre located in the US, for company X, secured via encryption with regularly rotating keys, kept separately from the workload).

[70]Wolff/Brink/v. Ungern-Sternberg / *Spoerr*, Art. 30 DSGVO, para 6; Ehmann/Selmayr / *Bertermann*, Art. 30, para 8; Kühling/Buchner / *Hartung*, Art. 30 DSGVO, para 15.

[71]Paal/Pauly / *Martini*, Art. 21 DSGVO, para 5; Ehmann/Selmayr / *Bertermann*, Art. 30, para 9; Kühling/Buchner / *Hartung*, Art. 30 DSGVO, para 15.

activity, with the added information that it ends and is re-started annually.

Since the legislator has not given any specific guidance as to the limits of such a bundling, it should probably be considered that the question of how to structure the processing activities can be left more or less to the discretion of the controller, as long as all the elements listed in Article 30(1) are equal (same controller, purpose, types of affected data, recipients etc.), or at least sufficiently similar so that they can be summarised together, and the principles of transparency and accountability are being adhered to.[72] This again shows how generally flexible the term "processing activity" is applied. This is even more so underlined by the fact that it is not necessarily used consistently throughout the GDPR.[73] In general, however, as has been shown above, it will be applied in order to underline that a specific processing is meant or alternatively when referring to a similar type or category of processing.

c) Automated Means

As per the definition found in Article 4 No. 2 GDPR, processing includes any operation performed on personal data whether or not by automated means, thereby clarifying that manual processing also falls under the Regulation. This "clarification" seems slightly unnecessary considering the broad scope of the term "processing" and was therefore most likely only added in order to avoid misunderstandings, as "data" might intuitively be associated with technical operations and procedures.[74] Consequently, purely paper-based activities such as keeping files in a cabinet, collecting business cards, taking notes, or simply throwing away documents containing personal data will also be considered processing.

---

[72]Ehmann/Selmayr / *Bertermann*, Art. 30, para 9.

[73]For more details see: *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 30 DSGVO, para 16.

[74]Kühling/Buchner / *Herbst*, Art. 4 Nr. 2, para 16.

It should however be noted that Article 2(1), which concerns the material scope of the Regulation, puts certain limitations on its applicability, stating that it applies to non-automated processing only where the data in question forms or is intended to form "part of a filing system". A filing system on the other hand, as per Article 4 No. 6 GDPR *"means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis"*.[75] The reasoning behind including structured data within the scope of the application is the idea that paper files, if organised well, can make finding information just as easy as it would be to simply search a database.[76] If therefore manually processed data had been excluded from the scope of the Regulation, this might have created a possibility for entities to circumvent its applicability by simply discarding certain very sensitive data points from automatic processing.[77] Conversely, this also demonstrates that unorganised manual processing is not really seen as a threat for the rights and freedoms of data subjects. The crucial elements of a "filing system" will therefore be the fact that it is *structured* and thereby *accessible*; these criteria will make the data found therein more easily attainable, resulting in a higher risk for data subjects.[78]

4. Personal Data

Last but not least, in order to identify the controller of a processing activity, we need to consider that the processing for which means and purposes are being determined has to relate to personal data. While this is probably obvious, it should perhaps still be mentioned that this definition is not only crucial for the denomination of the

---

[75]On a side note, this definition mirrors exactly the definition of "personal data filing system", contained in the Data Protection Directive, again showing how many of these concepts and ideas are not at all new in the realm of data protection.

[76]*FRA*, Handb. on EDPL, 100.

[77]This risk of circumvention is also being acknowledged in Recital 15, which derives from it the need for technological neutrality.

[78]*Voigt/von dem Bussche*, GDPR, 10.

controller but in fact the pivotal point of the whole General Data Protection Regulation. What also needs to be considered, as it relates specifically to the definition of the controller, is the fact that the entity in question must not be aware of the fact that it is processing personal data in order to be considered as such.[79] This means that even where a party wrongly believes that they are not processing personal data (for example due to failed anonymisation) they will still be subject to all obligations under the GDPR.

In accordance with Article 4 Nr. 1 GDPR: *"personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*. In order to provide a complete picture, each of these elements shall be analysed more closely in the subsequent passages.

a) Any Information

Similarly to the component of "any operation" in the definition of processing previously, the first defining characteristic of "personal data" essentially fulfils the function of underlining the very broad scope of application, showing that under the right circumstances, there are basically no limits as to what kind of information could be considered "personal".[80] Such an extensive understanding of the personal sphere of an individual is also in line with the interpretation of the European Court of Human Rights, which also applies a very broad definition of the term "private life".[81] While these terms are not

---

[79] *EDPB*, Guidelines 07/2020, para 41.

[80] *Art. 29 WP*, Opinion 4/2007, 6; Rücker/Kugler, *Rücker*, B. Scope of application, para 72; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 8; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 25.

[81] Amann v. Switzerland App no. 27798/95 (ECtHR, 16 February 2000), para 65: "*[...] the term "private life" must not be interpreted restrictively. In particular,*

equal,[82] it shows a certain tendency within the European legal realm to include areas such as work or public activities into the scope of the "personal".

It is also not necessary for information to be based in fact in order to be protected by the Regulation.[83] The legislator clearly foresaw the possibility that certain data points might be incorrect by granting the data subjects a right to rectification in Article 16. Information about an individual must also not be objective in order to be considered personal data. Subjective statements such as opinions or assessments of that person also fall under the scope of the regulation.[84] Relevant practical examples will typically include job references,[85] creditworthiness,[86] or the creation of online profiles.[87]

Furthermore, again corresponding with the principle of technological neutrality laid down in Recital 15, there are no restrictions with regards to the format in which information needs to

---

respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42). That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 [...]".

[82]The Charter of Fundamental Rights of the European Union contains both a right to respect of private and family life (Article 7 CFR) and a separate right to protection of personal data (Article 8 CFR).

[83]*Art. 29 WP*, Opinion 4/2007, 6; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 9; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 29; *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO, para 5.

[84]*Art. 29 WP*, Opinion 4/2007, 6.; Rücker/Kugler, *Rücker*, B. Scope of application, para 3; Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 16; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 10.

[85]Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 16.

[86]Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 10; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 29.

[87]*Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 35.

be kept.[88] Article 29 of the Data Protection Working Party in its Opinion 4/2007 on the concept of personal data states that *"the concept of personal data includes information available in whatever form, be it alphabetical, numerical, graphical, phytographical or acoustic, for example"*, thereby also explicitly including images and sounds.[89] Such an inclusion of various formats was not only logical but in fact necessary considering the existing possibilities of automatic processing, as well as the rapid developments in areas such as voice and facial recognition.[90]

b) Relating to

The information in question must relate to an individual, meaning that it needs to be about that person.[91] While establishing the existence of such a relation might be quite simple and straightforward in some instances, for example, where a name or other direct identifier is attached to a file or other compilation of information, there are as well a multitude of scenarios where it will be more difficult to determine whether or not a certain data point is in fact connected to a natural person. This might be the case where information is clearly related to an individual but it is not clear to whom it belongs (lost notebook or diary), where data is related to an object but information about an individual might be drawn from it (worth of a car, jewellery, house, or other belongings) or where data clearly relates to a different person but information about a certain individual might also be drawn from it (medical records regarding hereditary diseases). In order to determine whether such data could be considered as

---

[88]Ustaran / *Macmillan,* Chapter 4, 73; Rücker/Kugler, *Rücker*, B. Scope of application, para 75.

[89]*Art. 29 WP*, Opinion 4/2007, 7.

[90]*EDPB*, Guidelines 3/2019, para 2ff; *EDPB*, Guidelines 02/2021, para 1-6; *Nautsch and others*, INTERSPEECH 2019, 3695, 3698.

[91]*Art. 29 WP*, Opinion 4/2007, 9; Ustaran / *Macmillan,* Chapter 4, 73; Rücker/Kugler, *Rücker*, B. Scope of application, para 76.

"relating to" an individual, the Art. 29 WP suggests that one of the following elements needs to be present: content, purpose, or result.[92]

aa) Content

The content element is the most obvious and straightforward. Information relates to a natural person, if it is *"about that person"*.[93] In those instances, the data will most likely be directly marked as relating to a person. For example, all the information contained in an account or folder of a certain client or employee will relate to that individual. The same goes for statements made directly about an individual, such as "This is the car of X" or "X likes red wine",[94] as well as the content of any identity document.[95] Due to the clear identification, these types of data will be considered as relating to a person regardless of any other elements, such as the circumstances, intent or purpose.[96]

bb) Purpose

The purpose element, on the other hand is realised where data is being used *"with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual"*.[97] This element therefore specifically asks for the overall circumstances surrounding a specific situation to be taken into account.[98] Purpose alone without the element of content would typically come into play where data is relating to an object, rather than a subject. A textbook example would be call logs from a work phone, which technically relate to an object (the phone), but could at the same time be used to find out information relating to both the person using the phone, as well as

---

[92] *Art. 29 WP*, Opinion 4/2007, 10.

[93] ibid.

[94] Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 10.

[95] *Art. 29 WP*, Opinion 4/2007, 10.

[96] Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 14.

[97] *Art. 29 WP*, Opinion 4/2007, 10.

[98] *Art. 29 WP*, Opinion 4/2007, 10; Wolff/Brink/v. Ungern-Sternberg / *Schild*, Art. 4 DSGVO, para 24.

those calling (or even not calling) them.[99] The differentiation can also be illustrated by using the above-mentioned statements "This is the car of X" and "This is the house X lives in". While these two sentences clearly constituted personal data and fulfilled the element of content, this would not be the case if they were changed to: "This car costs Y amount of Euros" and "This house in infected by mould". Both of these sentences refer to an object and do not, in of themselves, contain any personal data. If, however, we know to whom a certain car belongs or where they live, it could be used in order to make certain evaluations regarding that individual, such as, for example, their creditworthiness or health status. Such information is used on a regular basis by banks and insurance providers and does constitute personal data, if used for purposes related to an individual.

cc) Result

Last but not least, we can use the element of result in order to determine whether or not a set of information relates to a natural person. This element will be present where, in consideration of the overall circumstances, certain data is likely to be used in a manner which would have an impact on the rights and interests of an individual.[100] This effect, however, is not to be interpreted in the meaning of Article 22(1) or Article 35(3)(a), which discuss legal or similarly significant effects. It refers to any sort of ramification for the individual, including the mere fact that they are being treated differently than others as a result of the processing.[101] Article 29 Working Party provides in its Opinion the example of monitoring a taxi's position via satellite in order to assign the closest car to each client.[102] Neither the content nor the purpose of the processing relate to an individual. The content itself relates to an object: the car, while

---

[99] *Art. 29 WP*, Opinion 4/2007, 11; Rücker/Kugler, *Rücker*, B. Scope of application, para 79; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 13.

[100] *Art. 29 WP*, Opinion 4/2007, 11; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 14.

[101] *Art. 29 WP*, Opinion 4/2007, 11.

[102] ibid.

the purpose is purely economic. The company simply wants to save costs on fuel and achieve greater customer satisfaction through providing a fast service. At the same time, this information could be used in order to monitor the action of the drivers, how fast they drive, how efficiently, and whether they adhere to the speed limits. This use of the information could therefore have a significant effect on the driver if it was used in order to check on their working habits or handed over to the police. It will, therefore, still be considered as "relating to" that individual.

It is important to underline that while in many instances all of these elements might be present and intertwined with each other, it is sufficient for one of these to be fulfilled in order to satisfy the characteristic of "relating" to a person.[103] The inclusion of information relating to objects again shows a high level of diligence on the side of the lawmakers in trying to assure complete and exhaustive protection for the rights and freedoms of each individual. It should, however, be noted that while data points relating to objects may often, though the elements of purpose and result, constitute personal data, there is a certain degree of individuality and level of detail that needs to be attached to that object so that it can be considered as uniquely applying to an individual.[104] As exemplified previously, information about a car or a phone can give us a lot of data regarding the owner or primary user but this will not be the case in instances where it is being used by an unspecified and uncontrolled number of people. This also again underlines the ambiguity of these terms and the importance of always considering the overall circumstances of each case.[105]

---

[103] *Art. 29 WP*, Opinion 4/2007, 11; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 14; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 11.

[104] *Krügel*, 10 ZD 2017, 455, 457; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 13.

[105] *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 22; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 13; Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 16; *Krügel*, 10 ZD 2017, 455, 457.

c) Identified or Indentifiable

In order for data to be considered "personal data", the person to which the information is related needs to be identified or identifiable.

aa) Identified

Neither Article 4 No. 1, nor any of the recitals contain details on when a person is to be considered as "identified". According to the Opinion of Art. 29 WP, a person should qualify as "identified" if *"within a group of persons, he or she is "distinguished" from all other members of the group"*,[106] again not adding many details to the terminology. While the reasoning behind this lack of attention might lie in the fact that there is no legal consequence to the differentiation between "identifiedness" and "identifiability", making the distinction practically irrelevant,[107] a difference must nonetheless exist if the lawmakers decided on such a wording and should therefore not be overlooked. It can be assumed that in contrast to the attribute of "identifiability", the term "identified" means an action that is completed and that therefore there are no additional steps or reflections required in order to determine the concrete identity of an individual. The identity of the data subject would therefore need to be contained directly within the information in question.[108] Consequently, the question whether or not a person is in fact identified should, in most instances, be straightforward and easy to answer.

bb) Identifiable

The same can unfortunately not be said about the feature of "identifiability" as the presence (or lack of such) is on a regular basis

---

[106] *Art. 29 WP*, Opinion 4/2007, 12.

[107] Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 9.

[108] Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 18; Rücker/Kugler, *Rücker*, B. Scope of application, para 83.

the cause of much uncertainty.[109] Art 4 No. 1 of the GDPR specifies that *"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*.

Direct identifiability occurs where the provided information in itself is sufficient to establish the identity of a person.[110] This can result from the fact that an identifier is so unique that it only relates to one individual, which is the case for biometric identifiers such as fingerprints, DNA, or retinal scans and most identification numbers such as a person's personal ID, tax ID, or social security number. It can, on the other hand, also be a consequence of the overall circumstances or multitude of provided data points. For example, the most typically used direct identifier "name" will actually only act as one under certain circumstances or in combination with additional information. The possibility of globally, uniquely identifying someone solely by being given a name (even in combination with a surname) is almost impossible. In a specific situation such as meeting or conference, simply calling out someone's name will, on the other hand be sufficient to distinguish that individual from others. The same can be said, regardless of context, about data points consisting of a number of factors which overall allow direct identification such as name and address or a name and date of birth. Each of these factors on its own would not necessarily facilitate identifiability but together they constitute information through which a data subject can be directly identified.

This concept of identifying an individual through the combination of different data points leads us right into the question of what is indirectly identifiable, since it is here where the topic will unfold its full

---

[109] *Hofmann/Johannes*, 5 ZD 2017, 221, 221: *Brink/Eckhardt*, 5 ZD 2015, 205, 205; *Bergt*, 8 ZD 2015, 365, 365.

[110] *Art. 29 WP*, Opinion 4/2007, 13; Sydow/Marsch / *Ziebarth*, Art. 4, para 17; *Voigt/von dem Bussche*, GDPR, 11.

meaning and importance. In many (if not most) circumstances, the available information will in fact not seem to be sufficient to facilitate the identification of an individual but this will still be possible either based on the uniqueness of the combination of data points at hand or through the use of additional information.[111] These instances of indirect identifiability can and have caused major difficulties and sparked many discussions regarding the differentiation between personal and non-personal data points.[112] Therefore, these should be analysed in more detail below.

(1) Means of Identification

Recital 26 of the GDPR provides some clarification in that regard, specifying that when determining whether or not certain data is to be considered personal *"account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person"*. The Recital goes on to say that in order to define what is to be considered "reasonably likely", all factors at hand should be taken into account, *"such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments"*. The Recital, therefore, seems to generally opt for a risk-based and practical approach, specifying that a purely theoretical possibility of identification would not suffice if it is not reasonably likely to be achieved.

---

[111] *Art. 29 WP*, Opinion 4/2007, 13; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 19; *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO, para 7; Sydow/Marsch / *Ziebarth*, Art. 4, para 21ff; *Purtova*, 10 L.I.T. 2018, 40, 46; *Krügel*, 10 ZD 2017, 455, 456.

[112] *Krügel*, 10 ZD 2017, 455, 456; *Nink/Pohle*, 9 MMR 2015, 563, 563; *Sarunski*, 40 DuD 2016, 424, 424ff; *Boehme-Neßler*, 40 DuD 2016, 419, 419ff; *Purtova*, 10 L.I.T. 2018, 40, 46ff; *Finck/Pallas*, 10 IDPL 2020, 11, 14; C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779, para 31-49.

(a) Perspective

Whether relative or absolute criteria are to be used in order to establish the *"reasonable likeliness"* of identification has already been heavily discussed under the old Data Protection Directive[113] and is still subject to debate.[114] In accordance with the relative approach, the question of identifiability should always be answered from the perspective of the specific data holder, meaning that whether or not a specific dataset would be considered as "personal data" would solely depend on the means available to that entity.[115] This understanding, however, clearly goes against the wording of Recital 26, which verbatim includes "used by another person" into the scope of the interpretation, thereby showing that at least the relative approach in its pure form does not lie in the intention of the lawmakers.

Supporters of the absolute approach, on the other hand, believe that a data point would be considered as relating to a natural person as soon as a connection to an individual could presumably be made by anyone, not just the person holding the data.[116] As mentioned above, the literal reading of Recital 26 could suggest the support for this interpretation.[117] This other person would, however, also have to be reasonably likely to perform such an identification, given the circumstances. If theoretical identification by anyone, even individuals with no connection to the controller and no possible access to the dataset, would suffice, then the term would become

---

[113] *Bergt*, 8 ZD 2015, 365, 366-369; *Voigt*, 6 MMR 2009, 377, 378f.

[114] *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO, para 7; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 17; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 26; *Voigt/von dem Bussche*, GDPR, 12.

[115] Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 25; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 59; *Voigt*, 6 MMR 2009, 377, 379; *Hornung*, 28 DuD 2004, 429, 430.

[116] *Voigt*, 6 MMR 2009, 377, 378; *Brink/Eckhardt*, 5 ZD 2015, 205, 205f; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 58.

[117] *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO, para 7; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 26.

limitless and cover all eventualities. Under this definition, owning a store with second hand clothing would be considered a major processing operation since potentially the mother or best friend of the previous owner of a certain piece could come in and know who it belonged to. The same would then go for any object touched by another individual, as theoretically, the fingerprints left thereon could be traced back. While numerous examples such as these could be given,[118] these are obviously ridiculous and only underline that, just as the relative approach, the absolute interpretation of *"reasonable likeliness"* does not lead to satisfactory results.

Due to the amount of practical problems stemming from both of these theories, a number of corrective interpretations have developed in academia, which opt for either a generally relative or absolute view but always take into account corrective elements from the other position.[119] A similar hybrid approach has been taken by the European Court of Justice in its ruling on the case of *Breyer.*[120] Here, the court pointed out that the additional data which would be necessary in order to identify the data subject does not need to be held by a specific entity in order for the dataset in their possession to be qualified as personal data in the meaning of the directive.[121] On the other hand, it was also made clear that it would have to be reasonably likely for the entity in question to come into possession of that additional information.[122] In the case of *Breyer*, which concerned the qualification of dynamic IP addresses held by a media service provider, the court decided that since the provider would be able to contact a competent authority in order to obtain information facilitating the identification of individuals in the case of cyberattacks, the IP addresses registered with them would be considered personal data as the described process might not take place on a regular basis

---

[118]For more you may also refer to: *Purtova*, 10 L.I.T. 2018, 40, 58f.

[119]*Bergt*, 8 ZD 2015, 365, 365-368; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 60.

[120]C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779.

[121]ibid para 44.

[122]ibid para 45f.

but is in fact foreseen by law and thereby to be considered "reasonably likely".[123]

This shows that the decisive part of the question to what extent the possibility of identification through information held by another party affects the aspect of "identifiability" depends largely on the relationship between the different actors at hand. Although Recital 26 does not contain any specification or requirements as to who "another person" could be and whether or not it needs to have any sort of connection to the controller, it can be assumed that at least "processors", "recipients" and "third parties" in the meaning of Article 4 No. 8, 9 and 10 respectively should be included.[124] Based on the requirement of "reasonable likeliness" and in consideration of the views presented by the CJEU in the case of *Breyer* (as analysed here), we would need to conclude that while there is no formal requirement for any sort of connection, legal or otherwise, between a controller and another party, from a purely practical perspective there would have to be some sort of link facilitating the exchange or acquisition of information in any way, as otherwise identification would not actually be achievable.

For the media service provider, the CJEU established this link in the form of a legal provision, allowing them to obtain the information necessary to facilitate identifiability in the case of cyberattacks.[125] Similarly, a link will most likely always exist between a controller and a processor, since the latter is acting on behalf of the first. This is why for example, even strongly pseudonymised or encrypted datasets are still considered as identifiable if one of these parties is holding the means to re-identify the individuals behind them, because not only are both parties aware of the existence of these additional details but also at least the controller will, in most instances, be able to demand the handover of any dataset from the processor, including raw data, based on Article 28 (3) g), even where

---

[123]ibid para 47-49.

[124]Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 26; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 62.

[125]C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779, para 47.

the parties originally might have agreed on something else. If, on the other hand, no plausible connection can be made between the entity processing a dataset and the entity holding the additional information, the combination of the information becomes a purely fictitious and theoretical scenario and therefore the requirement for reasonable likeliness of identifiability will not be met.[126]

(b) Legality

Another question regarding the *"reasonable likeliness"* of identification concerns the legality of actions leading to the identification of a data subject. Since the ruling on the Breyer case put such a high emphasis on the legal channels of the media service provider in accessing the additional information required in order to connect the IP-addresses in their possession to a natural person,[127] some have started to wonder whether this means that the use of illegal means would as a rule be considered unreasonable.[128]

This interpretation can, however, not be followed for multiple reasons. First of all, the CJEU does not allude to the existence of such a restriction at any point. It simply provides reasons as to why in the particular circumstances at hand, the provider would be considered as having means by which a data subject could likely and reasonably be identified, which in the presented case are based in law. There is, however, no indication that the court intended to exclude actions prohibited by law from the scope of what may or may not be reasonably likely to occur. Such a reading would also verbatim contradict the Opinion of the Article 29 Working Party on the concept of personal data, which specifically asks for factors such as risks of organisational disfunctions, such as breaches of confidentiality and

---

[126] *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 63; Wolff/Brink/v. Ungern-Sternberg / *Schild*, Art. 4 DSGVO, para 18.

[127] C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779, para 47-49.

[128] *Finck/Pallas*, 10 IDPL 2020, 11, 18; *Purtova*, 10 L.I.T. 2018, 40, 64; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 29; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 64.

technical failures, to be taken into account.[129] Last but not least, the addition of such a stipulation would simply not make any sense if we consider one of the key changes the GDPR set forth: The explicit introduction of the concept of pseudonymisation, including a clear emphasis on the fact that pseudonymised data is still unequivocally to be considered personal data.

(2) Anonymisation

Excluded from the term "personal data" is information which has been anonymised. This clarification can be found in Recital 26 which states that the *"principles of data protection should [...] not apply to anonymous information"*, which is defined as information that "*does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"*. This is most commonly achieved through the techniques of generalisation and randomisation.[130]

(a) Randomisation

Randomisation refers to techniques which alter the veracity of the information so that the strong link between the data and the individual is removed.[131] The easiest way of achieving this result would simply be the deletion of certain data points which are crucial for the creation of a link between the information and the natural person.[132] Another alternative would be the modification of certain attributes, making these less accurate and thereby hindering the identification but still keeping the information intact to a certain extent, referred to as

---

[129]*Art. 29 WP*, Opinion 4/2007, 15.

[130]*Art. 29 WP*, Opinion 4/2007, 12-19; *Winter/Battis/Halvani*, 11 ZD 2019, 489, 490; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 34; *Hölzel*, 42 DuD 2018, 502, 503f.

[131]*Art. 29 WP*, Opinion 4/2007, 12; *DPC*, Guidance on Anonymisation, 11.

[132]*Winter/Battis/Halvani*, 11 ZD 2019, 489, 490; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 34.

"noise addition".[133] A special form of noise addition, called "permutation" may also be applied. Here the relevant values of the certain attributes are shuffled, artificially linking some of these to specific data subjects.[134]

(b) Generalisation

The second type of anonymisation technique is called generalisation and refers to the practice of generalising or diluting relevant attributes through the modification of their scale or magnitude.[135] This can, for example, be achieved through aggregation or ensuring that identical values are being shared with a certain number of other individuals (k-anonymity).[136] In that sense, aggregated and statistical data are generally excluded from the scope of the Regulation.[137] Also commonly used is the introduction of interval values (providing a certain range of values such as, for example, a range of ages, dates, heights or wages) and superordinate categories.[138]

(3) Pseudonymisation

Whereas the anonymisation of a dataset renders it no longer identifiable, excluding it both from the scope of personal data and correspondingly from the applicability of the GDPR as a whole, the same does not hold true for information which has been pseudonymised. Pseudonymisation refers to the practice of replacing one attribute within a record by another.[139] Commonly used techniques include

---

[133] *Art. 29 WP*, Opinion 05/2014, 12; *DPC*, Guidance on Anonymisation, 11.

[134] *Art. 29 WP*, Opinion 05/2014, 12; *DPC*, Guidance on Anonymisation, 11.

[135] *Winter/Battis/Halvani*, 11 ZD 2019, 489, 490; *Art. 29 WP*, Opinion 05/2014, 16.

[136] Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 34; *Art. 29 WP*, Opinion 05/2014, 6.

[137] Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 15.

[138] *Winter/Battis/Halvani*, 11 ZD 2019, 489, 490; *Art. 29 WP*, Opinion 05/2014, 16; *DPC*, Guidance on Anonymisation, 12.

[139] *Art. 29 WP*, Opinion 05/2014, 20; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 19; Rücker/Kugler, *Rücker*, B. Scope of application, para 99.

encryption, hash-functions, key-hash functions, and tokenisation.[140] Since all of these, however, still allow the re-identification of a natural person through the use of additional information such as encryption keys or in combination with the original dataset, data would still be considered as "identifiable". This is also confirmed by Recital 26 which stipulates that pseudonymised personal data should still be considered as information relating to an identifiable natural person. Similarly Recital 78, which provides examples of appropriate technical and organisational measures, lists "pseudonymising personal data as soon as possible" as one of those, again confirming that it should be considered only as a security mechanism but cannot remove the characteristic of identifiability.[141]

The differentiation between pseudonymised and anonymised personal data is not only highly relevant in practice, but will be of particular importance in the context of Personal Information Management Systems and the designation of their roles under the GDPR. While some PIMS include in their marketing the promise of only transferring or sharing anonymised information with the end recipients,[142] assuring true anonymisation will, in practice, not only be extremely difficult but arguably nearly impossible. As has been outlined before, the existence of a connection between an entity holding additional information and the one processing the data in question is extremely relevant for the determination of the reasonable likeliness of identifiability. Here it was concluded that although Recital 26 does not contain any specification as to who "another person" could be, it should be assumed that at least "processors", "recipients", and "third parties" in the meaning of Article

---

[140] *Art. 29 WP*, Opinion 05/2014, 20f.

[141] Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 19.

[142] See for example: MyDex, 'Achieving Transformation at Scale' (April 2021) 9, https://mydex.org/resources/papers/AchievingTransformationAtScale/AchievingTransformationatScaleMydexCIC-2021-04-14.pdf (accessed: 14 October 2025).

4 Nr. 8, 9 and 10 respectively should be included.[143] Depending on the respective designation of the legal function taken by PIMS and the data recipient, it might therefore be essentially legally impossible for the PIMS to transfer "anonymised" personal data, as long as they are still able to re-identify the individual user, especially if they were to be considered a processor or joint controller of the recipient.

d) Natural Person

Finally, yet importantly, Art. 4 No. 1 of the General Data Protection Regulation provides that the term "personal data" should only cover information relating to a natural person. This essentially leads to the exclusion of two groups: legal persons and the deceased.[144] For both of these categories there might, however, be circumstances under which information falling under such would still be included within the scope of Art. 4 No.1.

In the case of legal entities, this will be the case in which information concerning a legal person also allows for assumptions about an individual to be made, for example, concerning their financial circumstances or profession.[145] This will be particularly prevalent where a company only has one owner or shareholder.[146] Similarly, the data of someone who dies might still be considered as "personal data" of another living individual, where it allows for information about such to be derived from the data of the

---

[143]Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 26; *Karg* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 1 DSGVO, para 62.

[144]*Art. 29 WP*, Opinion 4/2007, 22f; Kuner and others / *Bygrave/Tosoni*, Art. 4(1), 103, 111f; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 13f; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 3f.

[145]*Art. 29 WP*, Opinion 4/2007, 23; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 14.

[146]Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 3; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 14; Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECLI:EU:C:2010:662 para 53; Kuner and others / *Bygrave/Tosoni*, Art. 4(1), 103, 111.

deceased.[147] This will, for example, apply in the context of information concerning hereditary diseases or other genetic data.[148] In the same vein, information about possessions belonging to a dead individual might allow for certain inferences or calculation to be made regarding the future financial status of their heirs. It should also be noted that while the data of deceased individuals is not protected under the GDPR, Member States are still free to extend the protection and scope of their national data protection laws towards this group, which has, for example, been done by Denmark and Italy.[149] Furthermore, largely dependent on national legislation is the extent to which unborn children are protected by the GDPR, since this is where the legal status of the nasciturus will be determined.[150]

III. Pluralistic Element

Art. 4(7) GDPR also states that the determination of the purposes and means of the processing of personal data can be done alone or jointly with others. This element does not fully define the term of the controller in any substantive way but is only there to clarify that there can be multiple controllers for one processing activity. The idea of joint controllership in itself is not new, since as already mentioned, the definition found in Art. 4(7) GDPR has been directly lifted from Art. 2(d) of the Data Protection Directive. What is new, however, are the various rules and conditions for joint controllership which have been laid down in Art. 26 GDPR. These, as well as the many difficulties and complications that come with this legal figure, will be discussed in detail under Part 2 Chapter 3: C. Joint Controllers.

---

[147] *Art. 29 WP*, Opinion 4/2007, 22; Kühling/Buchner / *Buchner/Kühling*, Art. 4 Nr. 1 DSGVO, para 4; Rücker/Kugler, *Rücker*, B. Scope of application, para 109.

[148] Kuner and others / *Bygrave/Tosoni*, Art. 4(1), 103, 112; *Art. 29 WP*, Opinion 4/2007, 22; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 13.

[149] Kuner and others / *Bygrave/Tosoni*, Art. 4(1), 103, 112.

[150] *Art. 29 WP*, Opinion 4/2007, 23.

IV. Functional Element

A crucial component for the understanding of the legal designation of responsibility under the GDPR is the so called "functional element" applicable to all of these roles. While this characteristic cannot be derived from the formal wording defining the role of the controller, it has been established and strongly supported by most official guidelines and literature, as well as the CJEU.[151] This element is realised through two main components. First of all, as has already been remarked in multiple contexts previously in this text, the legal status of the parties is to be determined based on their actual influence and activities with regard to the processing of personal data and cannot be changed through formal designation, which would contradict the factual circumstances.[152] This focus on the true circumstances of the case is, however, to a certain extent adjusted by the idea of assuring the purposes of data protection are being met to the fullest extent.[153] The EDPB notes in that context that the *"concept of controller should be interpreted in a sufficiently broad way so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules"*.[154] The same understanding has been supported by the CJEU, which repeatedly highlighted that the concepts are not only to be understood in a functional manner but also broadly in order to assure *"effective and complete protection of data subjects"*.[155] In that sense, the determination of the respective roles and responsibilities takes

---

[151] *Bassini*, BLP 2019, 103, 107f; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 148; *EDPB*, Guidelines 07/2020, para 12; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 88; *Berger/Eisendle*, 15 IJLT 2019, 20, 24.

[152] Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 148; *EDPB*, Guidelines 07/2020, para 12; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 88; *Berger/Eisendle*, 15 IJLT 2019, 20, 24.

[153] Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 148.

[154] *EDPB*, Guidelines 07/2020, para 14.

[155] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 34; Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 28; Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 65–66.

place in consideration of the function of the law itself as well. Based on such an understanding, it is imaginable that there might be instances in which formally speaking not all previously outlined elements for the consideration as a data controller might be present. However, an entity could still be designated as such if otherwise the rights and freedoms of the individual would be seriously endangered. In a sense, formal requirements and criteria are thereby to a certain extent set aside for the purpose of functionality.[156]

V. Case Law of the Court of Justice of the European Union

Additional details on how all of the elements of the term "controller" are to be interpreted can be drawn from the case law of the CJEU.

1. Google Spain

Probably the most central judgement in that regard is the decision in the case of *Google Spain v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, commonly referred to as *Google Spain*.[157]

a) Facts of the Case

Mario Costeja González, a Spanish national resident, issued a complaint against the publisher of the newspaper "La Vanguardia" La Vanguardia Ediciones SL, as well as Google Spain and Google Inc., with the Spanish Data Protection Authority, the Agencia Española de Protección de Datos (AEPD) in March 2010.[158] He opposed the fact that when entering his name, Google's search engine would offer links to two articles of the newspaper published on January 19, 1998 and March 9, 1998, which contained announcements regarding real estate auctions related to

---

[156]*Bassini*, BLP 2019, 103, 108.
[157]Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.
[158]ibid para 14.

proceedings for the recovery of social security debts.[159] Since the attachment proceedings concerning him had by the time been fully resolved for several years, he considered the reference to be irrelevant and requested 1) La Vanguardia to be required to remove or alter the articles so that personal data concerning him would no longer be visible or alternatively to make use of available tools protecting that information; and 2) Google Spain or Google Inc. to be required to remove or conceal his personal data so that it would no longer appear in the search results and the links to La Vanguardia.[160]

b) Course of the Proceedings

The Spanish DPA rejected the complaint with regards to the demands put forward against La Vanguardia, concluding that the publication of the details regarding the auctions was legally justified since it took place upon order of the Ministry of Labour and Social Affairs and had the intent of assuring a high level of publicity in the interest of securing a large amount of potential bidders.[161] Mr. Costeja González's request concerning the concealing or removal of his personal data by Google Spain and Google Inc. was, however, upheld.[162] Here the AEPD took the stance that operators of search engines can be obliged to withdraw certain data points or the prohibited from accessing such, where the processing of personal data would *"compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties"*.[163] The DPA also supported the notion that such requirements may be put forward against search engine operators independently and regardless of the validity of the information contained on the underlying web page.[164]

---

[159]ibid para 14.
[160]ibid para 15.
[161]ibid para 16.
[162]ibid para 17.
[163]ibid para 17.
[164]ibid para 17.

Both Google Spain and Google Inc. subsequently brought separate actions against that decision before the Spanish National High Court (Audiencia Nacional).[165] The Court decided to join the actions since it considered that they raised questions concerning the data protection obligations of search engine operators in general, as well as the correct interpretation of the Data Protection Directive in the context of these "new" technologies.[166] Based on that, the High Court decided to stay the proceedings and referred a number of questions to the Court of Justice of the European Union for preliminary ruling. These questions concerned, among other things, terms such as "establishment", "use of equipment", and "processing of personal data", as well as the extent of the right to erasure and blocking of data.[167]

c) Judgement

While all of these points are of central importance in the context of the protection of personal data and the case is most famously known for the development of the so called "right to be forgotten",[168] the analysis of the Judgement should at this point focus on the considerations with regards to the term "controller" examined in this section. In that context, the CJEU first established that the automatic, constant, and systematic exploration of the content found online in search of information is to be considered as the collection, retrieval, recording, and organisation of personal data.[169] In the same vein, the presentation of the relevant search results to online users can be regarded as a disclosure or "making available" of personal data.[170] Conversely, the processing of personal data conducted by a search

---

[165]ibid para 18.

[166]ibid para 18f.

[167]ibid para 20.

[168]*Holznagel/Hartmann*, 4 MMR 2016, 228, 228, *Buchholtz*, 12 ZD 2015, 570, 573-577; *Arning/Moos/Schefzig*, 30 CR 2014, 447, 447ff; *Bunn*, 31 CLSR 2015, 336, 336ff.

[169]Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 28.

[170]ibid para 28.

engine constitutes a processing activity separate from that conducted by website operators, for which both the means and purposes are being determined by the search engine, thereby making them the controller.[171]

The court also pointed out that search engines play a decisive role in the distribution and dissemination of information, making it easier to find and access such.[172] Especially when users conduct searches on individual names, the presentation of both accurate and well-organised lists of results can lead to the creation of quite detailed personal profiles of certain data subjects.[173] In that sense, operators such as Google can significantly impact the individual's privacy and should therefore be responsible for the assurance of all relevant guarantees required by the law for their protection.[174] Therefore, excluding search engine operators from responsibility under data protection law could potentially seriously hinder the *"effective and complete protection of data subjects"*, which is supposed to be ensured through the introduction of a broad definition of "controller".[175]

d) Conclusions

The findings of the court again underline the previously mentioned "functional element" of the definition of "controller" under the GDPR, supporting the notion that the term needs to be interpreted in a manner which allows for the rights and freedoms of the individual to be protected as fully, effectively, and completely as possible. The analysed considerations also demonstrate the importance of differentiating between different processing activities being performed for different purposes on the same set of personal data, since here the search engine operator, established to be a controller,

---

[171]ibid para 33, 35.
[172]ibid para 36.
[173]ibid para 37.
[174]ibid para 38.
[175]ibid para 34.

did not create, collect, or publish any new information but simply in a sense re-structured and re-organised in order to allow easier retrievability, thereby initiating a new processing activity altogether. It should also be noted, that while the court's clear focus lay in confirming the responsibility of Google as the data controller, the court did leave open the possibility for considering joint controllership with the website operators, based on the fact that these are given the option of indicating to the search engine that certain information should be excluded from the automatic indexing though the implementation of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive'.[176] While so far in practice joint controllership between search engine and website operators is not assumed, the court's reflections in that regard again evidence the extreme complexity in delineating the respective roles and responsibilities of the involved parties. The differentiation between joint and separate controllers will therefore be analysed in more detail in the subsequent passages.

2. Other Cases

The CJEU has also published a number of other judgements dealing with the question of controllership in general, as well as the scenarios in which the means and purposes of the processing of personal data are being determined jointly with other parties. The most central landmark judgements in that regard are those in the cases of *Wirtschaftsakademie Schleswig-Holstein*,[177] *Jehovan todistajat,*[178] and *Fashion ID*.[179] Since the focus of these, however, lies in the determination of the applicability of joint controllership, they should be discussed in detail in the context of that term (see Part 2 Chapter 3: C. III. Case Law of the Court of Justice of the European Union).

---

[176]ibid para 39.
[177]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388.
[178]Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551.
[179] Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.

VI. Effect

Once it has been established that a certain legal or natural person is determining the means and purposes of the processing of personal data and therefore to be considered as the data controller under Art. 4 No. 7 of the GDPR, the question naturally arises what kind of effects such a designation has on an entity and what the potential results, responsibilities, and consequences in that regards might be.

1. Responsibility

Article 24 of the GDPR has been titled "Responsibility of the Controller" and therefore constitutes an important starting point for considering the legal consequences arising from this role. Paragraph (1) therein provides that such an entity should *"implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation"*. There are therefore two important tasks emerging from this sentence: First of all, the controllers need to ensure that all processing activities under their control are being performed in accordance with the GDPR and secondly, they need to be able to demonstrate such compliance.

a) Processing in Accordance with the Regulation

Art. 24 is to be considered as a very generalised norm, which in a sense overarches the entirety of the Regulation since it requires controllers to ensure the overall compliance of the processing of personal data under their control.[180] In that sense, it does not directly create any responsibility but simply reiterates and confirms specific responsibilities found throughout the entire text of the GDPR. These

---

[180]Eßer/Kramer/von Lewinski / *Kramer/Meints*, Art. 24 DSGVO, para 8; Kühling/Buchner / *Hartung*, Art. 24 DSGVO, para 9; Ehmann/Selmayr / *Bertermann*, Art. 24, para 1.

are numerous, since the entire objective of the GDPR is based in the assurance of free movement of personal data through the creation of rules assuring the protection of a natural person with regard to the processing of such (Art. 1(1) GDPR).

Listing each and every specific responsibility of the controller resulting from the Regulation would thereby more or less lead to a reproduction of the entire text and can therefore be considered excessive and unnecessary for the purpose of this thesis. In order to form a basic understanding of the extent of the requirements put on the controller, it should be sufficient to mention the essential elements in that regard. These are, for example, the adherence of each processing activity to the main principles of data protection outlined in Art. 5 (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability); the assurance of all data subject rights outlined in Chapter 3 (information, access, rectification, erasure, restriction, portability, objection, not to be subject to automated decision making); the maintenance of a record of processing activities (Art. 30); and of necessary measures for the security of personal data (Art. 32); as well as the performance of data protection impact assessments (Art. 35 and 36); and the reporting of breaches (Art. 33 and 34), where necessary.

b) Technical and Organisational Measures

In accordance with Art. 24(1), the technical and organisational measures which are to be implemented by the controller in order to ensure the compliance of a processing activity with the regulation, need to be appropriate. Such appropriateness is to be determined in consideration of the nature, scope, context, and purpose of the specific processing activity, as well as the likelihood and severity of the potential risks which might arise to the rights and freedoms of natural persons as a result of such. This is part of the risk-based approach, generally supported by the GDPR, in accordance to which responsible parties are prescribed to consider the criticality, circumstances, and consequences of a particular processing activity when determining what specific steps should be taken, rather than

giving them strict and inflexible rules, potentially resulting in disproportionate and excessive requirements.[181] As a consequence, controllers will need to perform a risk analysis prior to the commencement of any sort of processing activity.[182] Interestingly, the reference to the "cost of implementation" as a relevant criterion for assessing the appropriateness of certain measures, found in Articles 25(1) and 32(1) GDPR, is missing from Art. 24(1). This should, however, not be understood as an intentional exclusion, in the sense that compliance would need to be achieved "at all costs" but rather results from the more general, overarching character of the norm, the principles of which are then further detailed in other places, such as Art. 25 and 32.[183]

Article 24(2) also provides that such measures should also include the implementation of appropriate data protection policies by the controller where this would be proportionate in relation to the considered processing activities. The term "data protection policies" has not been defined in the GDPR, making it unclear what specifically such a policy should entail.[184] The term can also only be found in one other place within the Regulation, namely the definition of binding corporate rules contained in Art. 4 No. 20, described as *"personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity"*. It is therefore most commonly assumed that such policies represent a form of internal or external rules and guidance providing

---

[181]*Albrecht*, 2 CR 2016, 88, 93f; *Gellert*, in: Trends und Communities der Rechtsinformatik, 527, 527ff; *Gonçalves*, 23 J. Risk Res. 2020, 139, 139ff.

[182]Kühling/Buchner / *Hartung*, Art. 24 DSGVO, para 13; Ehmann/Selmayr / *Bertermann*, Art. 24, para 6.

[183]*Koós/Englisch*, 6 ZD 2014, 276, 278; Kühling/Buchner / *Hartung*, Art. 24 DSGVO, para 18; Ehmann/Selmayr / *Bertermann*, Art. 24, para 12.

[184]Kühling/Buchner / *Hartung*, Art. 24 DSGVO, para 21; Ehmann/Selmayr / *Bertermann*, Art. 24, para 16.

instructions and regulations for the handling of personal data within an enterprise.[185] Some sources have also considered the possibility of deriving a requirement to implement a data protection management system, in the sense of a compliance tool,[186] from this.[187] Taking into account the principle of proportionality, the existence of such a general obligation can, however, not be assumed. Controllers would rather be required to make decisions regarding the need for such, as well as their extent, comprehensiveness and level of detail dependent on the type of processing activities performed by a specific entity.[188]

c) Accountability

The requirement for controllers to be able to demonstrate that the processing under their control is being performed in accordance with the Regulation directly mirrors the principle of accountability enshrined in Art. 5(2), which also calls for the exact same, with regards to the compliance with the principles relating to the processing of personal data, contained in Art. 5(1).

aa) Innovation of Approach

This notion signifies an important change in the approach to data protection law within the EU. Under Articles 18 and 19 of the previously applicable Data Protection Directive, controllers were required to notify the relevant Data Protection Authorities (DPAs) prior to carrying out any type of processing activity. These notifications in a sense mirrored the record of processing activities which controllers have to keep under the GDPR (Art. 30 GDPR), as

---

[185]Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 24' DSGVO, para 19; Kühling/Buchner / *Hartung*, Art. 24 DSGVO, para 21.

[186]See Part 1 Chapter 1: A. III. Compliance Management.

[187]*Jung*, 5 ZD 2018, 208, 208-211; *Wichtermann*, 9 ZD 2016, 421, 422; E-ßer/Kramer/von Lewinski / *Kramer/Meints*, Art. 24 DSGVO, para 20f; *Thode*, 11 CR 2016, 714, 716.

[188]Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 24' DSGVO, para 21-23; Eßer/Kramer/von Lewinski / *Kramer/Meints*, Art. 24 DSGVO, para 34.

they had to contain details such as name and address of the controller, the purpose of processing, the categories of personal data and data subjects, recipients, intended third country transfers, as well as a description of technical and organisational measures implemented in order to assure the security of the processing operation. Considering the amount of processing of personal data being performed by large as well as small and medium enterprises on a regular basis, it should come without surprise that DPAs were largely unable to examine all of these notifications.[189] The requirement was generally considered as an unproportionate burden for businesses, as well as no longer in the spirit of modern times.[190] Additionally, it bore the risk of causing controllers to feel more secure with regards to the processing activity and, in a sense "discharged" from their responsibilities as a result.[191] In that sense, the current accountability based regime can definitely be considered as a necessary improvement.

bb) Forms of Demonstration

Article 24 does not provide detail as to how the compliance with the Regulation can be demonstrated, again evidencing its general character by which it in a sense overarches the more specific obligations found in other Articles. Some quite specific duties, potentially enabling the active demonstration of compliance can, however, be found within the text of the GDPR.

(1) Codes of Conduct and Certifications

The one specific form of demonstrating compliance, established by Art. 24(3), is the adherence to codes of conduct or certification mechanisms, approved in accordance with Articles 40 and 42 respectively. The Regulation provided that these *"may be used as an element by which to demonstrate compliance with the obligations of*

---

[189]Kuner and others / *Docksey*, Art. 24, 555, 560.

[190]*Albrecht*, 2 CR 2016, 88, 93; Ehmann/Selmayr / *Bertermann*, Art. 30, para, 1.

[191]Kuner and others / *Docksey*, Art. 24, 555, 560.

the controller". The wording, however, makes it clear that the utilisation of such is neither mandatory (*"may"*), nor exhaustive or final (*"as an element"*). In that sense, even where controllers are adhering to one of these mechanisms, data protection authorities will not be bound by the concluded results but rather, can still conduct their own internal investigations of the company's compliance level.[192] The relevance of this verifiability of pre-approved compliance mechanisms has, for example, been demonstrated in the context of the Privacy Shield and its predecessor Safe Harbour, both of which constituted data transfer mechanisms approved by the European Commission but were later deemed invalid by the CJEU.[193] In that sense, controllers are still advised to deploy alternative forms of demonstrating compliance. Recital 77, for example, also mentioned guidelines of the Data Protection Board and indications provided by a data protection officer as another valid alternative.

(2) Record od Processing Activities

Whereas Art. 24(3) only mentions two mechanisms of demonstrating compliance with the GDPR, it places certain duties on the controller which can also, to a large extent, serve that purpose. The most relevant in that context is probably the requirement to maintain a record of processing activities found in Art. 30, as it effectively allows the presentation of multiple other obligations under the Regulation, such as the performance of a DPIA, data processing contracts, or technical and organisational measures, by way of including details regarding those points in the ROPA.[194] Such an understanding is also supported by Recital 82, which explicitly states that the records of processing activities are to be kept in order to demonstrate compliance with the Regulation. Considering the

---

[192] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 24 DSGVO, para 26; Gola/Heckmann / *Piltz*, Art. 24 DSGVO, para 65.

[193] Case C-362/14 *Schrems* [2015] ECLI:EU:C:2015:650 and Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559.

[194] *Gossen/Schramm*, 1 ZD 2017, 7, 9f; Ehmann/Selmayr / *Bertermann*, Art. 30, para 2; *Thode*, 11 CR 2016, 714, 718.

amount of information contained in such, the access to them explicitly authorised by Paragraph 4 can be quite effective for Data Protection Authorities in order to gain a first general overview of the level of compliance with the Regulation within a specific entity.[195] Additionally, the prerequisite for such to be kept in writing (Art. 30(3)) assures that it can manifest the current state of the controller's processing operations in a form which is both permanent and accessible.[196]

(3) Other Forms

Other obligations outlined directly within the text of the GDPR, which can also be construed as being directed towards the assurance of accountability are, for example, stipulation such as the performance of Data Protection Impact Assessments (Art. 35), the designation of a Data Protection Officer (Art. 37), the notification of breaches to Data Protection Authorities (Art. 33), and the contractual regulation of the involvement of other parties in the processing of personal data (Art. 26 and 28). Additional forms of assuring accountability suggested within compliance literature, as well as directly by the authorities, include solutions such as: the adoption of internal policies and processes, the establishment of company-wide training and awareness campaigns for employees, performing internal and external audits, creating internal mechanisms for reporting in-compliance and violations of privacy, as well as designating individuals and teams responsible for the implementation and monitoring of data protection policies (additionally to the DPO).[197]

---

[195]Ehmann/Selmayr / *Bertermann*, Art. 30, para 2; Kühling/Buchner / *Hartung*, Art. 30 DSGVO, para 33

[196]Kühling/Buchner / *Hartung*, Art. 30 DSGVO, para 32.

[197]Kuner and others / *Docksey*, Art. 24, 555, 563f; *Thode*, 11 CR 2016, 714, 716; *Art. 29 WP*, Opinion 3/2010, 11-12; *Urquhart/Lodge/Crabtree*, 27 Int. J. Law Inf. Technol. 2019, 1, 9-12; https://www.edps.europa.eu/sites/default/files/publication/16-09-30_accountability_speech_en.pdf (accessed: 25 February 2026).

2. Consequences

As has been outlined above, the controller takes the central role when it comes to the responsibility for the processing of personal data under their control, as it is their obligation to assure the compliance of such with the GDPR while additionally being able to demonstrate such at any given time. This naturally leads to the question of the consequences which might result from this type of responsibility. These can broadly come in two forms: either measures imposed by the data protection authorities or direct liability for suffered damages towards individuals. Both of these will be outlined below.

a) Powers of Data Protection Authorities

Art. 58 provides supervisory authorities with a number of competences intended to enable them to efficiently carry out their tasks as outlined in Art. 57. These competences, referred to as "powers" have been divided into three categories: investigative powers, corrective powers, and authorisation and advisory powers.

aa) Investigative Powers

The investigative powers of the DPAs are outlined in Art. 58(1) and serve the purpose of allowing them to establish the relevant facts surrounding the processing of personal data by a controller or processor.[198] They include capabilities such as ordering the provision of information, carrying out investigations in the form of audits or reviews of certifications, and obtaining access to personal data, as well as the premises of the controller and processor. Since the Regulation does not provide for any specific instances under which these powers can be applied, it is generally assumed that authorities can make use of them at their discretion in accordance

---

[198]Paal/Pauly / *Körffer*, Art. 58 DSGVO, para 5; Kuner and others / *Georgieva/Schmidl*, Art. 58, 939, 946.

with the principle of proportionality and that it is not necessary for a specific indication of a potential misconduct to be present.[199]

bb) Authorisation and Advisory Powers

The powers of supervisory authorities outlined in Art. 58(3) predominantly serve the purpose of supporting all relevant actors in assuring an appropriate level of protection for the processing of personal data, in accordance with the requirements of the Regulation. In that sense, DPAs should provide advice to controllers where a data protection impact assessment indicates that the intended processing activity would result in a high risk and the measures established by the controller are not sufficient to mitigate such (Art. 58(3)(a)) and can authorise these activities where adequate (Art. 58(3)(c)). They are also compelled to issue opinions to parliaments, governments, other national institutions, and the public with regard to issues related to the protection of personal data (Art. 58(3) (b)). Additionally, supervisory authorities have a number of competences in the context of approving, opining on, and issuing compliance instruments such as codes of conduct, certifications and binding corporate rules (Art. 58(3)(d), (e), (f) and (j)). Finally, they can to a certain extent affect the validity of data transfers to third countries by adopting standard contractual clauses or authorising them and administrative arrangements between public authorities or bodies (Art. 58(3)(g), (h) and (i)).

cc) Corrective Powers

The last type of powers, which are of a corrective nature, is arguably the most relevant in terms of potential consequences to be endured by a controller. Whereas the investigative powers solely provide a basis for the authorities to determine the actual facts of the case and the authorisation and advisory powers concentrate on supporting businesses achieving compliance by establishing the

---

[199]Ehmann/Selmayr, *Selmayr*, Art. 58, para 11; Paal/Pauly / *Körffer*, Art. 58 DSGVO, para 5; Gola/Heckmann / *Nguyen*, Art. 58 DSGVO, para 3.

necessary means, corrective powers aim to enforce the rectification of potential infringements of the law.[200] This is why they will typically be acted upon as a result of the investigations conducted under Art. 58(1).[201] The potential consequences arising for controllers as a result of these powers are varying in severity, with some sources arguing that Art. 58(2) depicts those escalation levels by starting with the least intrusive and ending with the most drastic measures.[202] There are many forms in which those measures can be classified. The division used for the purpose of this thesis broadly categorises them into warnings and reprimands, orders, fines, and legal proceedings.

(1) Warnings and Reprimands

In accordance with Art. 58(2)(a) and (b), controllers can receive warnings from a supervisory authority where the conclusion has been reached that specific intended processing operations are likely to infringe the Regulation. Reprimands can also be issued where such an infringement has already taken place. These two instruments can be considered the least severe forms of action against the controller since they are not legally binding and can therefore also not be formally considered as sanctions.[203] Their purpose lies rather in making the controller aware of certain deficiencies and allowing such to correct them on their own. This might be especially reasonable when the potential or current infringement is rather mild and there is no reason to assume that it will be repeated.[204] They might also be used as a preliminary step before introducing more strict forms of intervention.[205]

---

[200] *Voigt/von dem Bussche*, GDPR, 209.

[201] Gola/Heckmann / *Nguyen*, Art. 58 DSGVO, para 13.

[202] *Dieterich*, 6 ZD 2016, 260, 261; Gola/Heckmann / *Nguyen*, Art. 58 DSGVO, para 18.

[203] Schwartmann/Jaspers/Thüsing/Kugelmann / *Kugelmann/Buchmann,* 'Art. 58' DSGVO, para 80, 86; *Voigt/von dem Bussche*, GDPR, 209.

[204] Schwartmann/Jaspers/Thüsing/Kugelmann / *Kugelmann/Buchmann,* 'Art. 58' DSGVO, para 86.

[205] Kühling/Buchner / *Boehm*, Art. 58 DSGVO, para 22.

(2) Orders

Article 58(2) provides for a number of orders which can be directed against the controller. These can concern the requirements: to comply with a data subject request (Art. 58(2)(c)); to bring processing operations into compliance with the GDPR (Art. 58(2)(d)); to communicate a personal data breach to the data subject (Art. 58(2)(e)); to temporarily limit or completely cease a processing activity (Art. 58(2)(f)); to rectify or erase personal data or restrict its processing (Art. 58(2)(g)); and to suspend data flows to a recipient in a third country or to an international organisation (Art. 58(2)(j)). By imposing such mandates onto the controller, the supervisory authority will thereby directly affect the processing activities conducted by such. This can also be done by withdrawing or ordering the withdrawal of certifications issued pursuant to Articles 42 and 43, which can be done based on Art. 58(2)(h). It should also be noted that Recital 148 establishes that the prior compliance or lack thereof with measures ordered against a controller or processor should be considered as a factor when determining the necessity of issuing a fine and its extent.

(3) Fines

The sanction typically most feared by controllers is the possibility of being fined. Article 58(2)(i) provides that supervisory authorities may, under certain circumstances, impose administrative fines, either in addition or instead of the other corrective measures provided for in Art. 58(2). While the option of financial penalties was already possible under the Data Protection Directive since Article 24 thereof obliged Member States to lay down sanctions to be imposed for infringement of data protection law and some did allow for fines to be issued, this particular mechanism has gained far more attention and significance since the GDPR came into force.[206] This can, to a large extent, be attributed to the significant increase in the potential

---

[206] *Dieterich*, 6 ZD 2016, 260, 264.

amount of such fines, which has been and continues to be the subject of extensive media coverage.[207] After all, the potential amounts of the administrative fines provided for in Article 83 are quite significant; as based on the type of infringement they can constitute up to €10 million , or in the case of an undertaking, up to 2% of the total worldwide annual turnover (Art. 83(4)) of the preceding financial year or even up to €20 million , or in the case of an undertaking, up to 4% of the total worldwide annual turnover (Art. 83(5) and (6)).

These high sums were most likely introduced in order to assure that the issued fines are, in fact, effective and dissuasive as is required by Art. 83(1). The same, however, also asks for the issued penalty to be proportionate, which is why the overall circumstances need to be taken into account by the relevant supervisory authority, including elements such as e.g., the nature, gravity, and duration of the infringement; its international or negligent character; actions taken to mitigate the damage suffered by data subjects; any relevant previous infringements; the degree of cooperation with the DPA; and the level of compliance with the orders previously issued by such (see: Article 83(2) and Recital 148 GDPR). Ultimately, the calculation of the specific amount is, however, left to the discretion of the supervisory authority[208] which is why the selection of a reasonable and consistent method for their calculation is subject to much debate.[209]

---

[207] https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/ (accessed: 25 February 2026); https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans (accessed: 25 February 2026); https://www.journalism.co.uk/news/first-party-cookies-get-legal-help-to-avoid-fines-/s2/a982617/ (accessed: 25 February 2026); https://www.csoonline.com/article/571963/european-nations-issue-record-11-billion-in-gdpr-fines.html (accessed 25 February 2026); https://www.cpomagazine.com/data-protection/e405-million-gdpr-fine-for-instagram-over-privacy-settings-for-underage-users/ (accessed: 04 March 2026).

[208] *EDPB*, Guidelines 04/2022, para 15.

[209] For more on the topic see for example: *Ruohonen/Hjerppe*, 106 Inf. Syst. 2022, 101876; *Saemann and others*, PoPETs 2022, 314, 314ff; *Faust/Spittka/Wybitul*, 3 ZD 2016, 120, 120ff; *Golla*, 34 CR 2018, 353, 353ff; *Thiel/Wybitul*, 1 ZD 2020, 3, 3ff.

(4) Legal Proceedings

Last but not least, Article 58(5) provides that supervisory authorities should be vested with the right *"to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation"*. While the specific form in which DPAs may exercise that right will be dependent on the legal regulation of the specific Member State since the GDPR obliged them to provide these powers to their respective supervisory authorities, it can still constitute a relevant form of pressuring the controller into compliance.

b) Liability

Whereas the previous section described the potential measures and sanctions which can be directed against controllers by the supervisory authorities, the following passages will describe liabilities towards other parties. In that context, Art. 82(1) provides persons with the right to receive compensation for any damages, whether material or non-material, they might have suffered as a result of an infringement of the regulation caused by the controller or processor. The stipulations under which businesses will be required to provide such renumeration will be discussed below.

aa) Elegibility

Before clarifying the details and extent of such compensation, the question arises as to who is even eligible to make such a claim. Art. 82(1) stipulates in that regard, such a right should be given to *"any person"* who has suffered damage as a result of an infringement of the Regulation. This wording is inherently broad, which is why a certain limitation of the scope of eligibility has been discussed.

(1) Limitation to Natural Persons

The first possible limitation discussed in literature concerns the question whether legal persons should also be able to make claims for compensations under Art. 82(1) or whether such a right should

be reserved for natural persons.[210] Proponents of such a limitation have argued that legal persons would be excluded based on the fact they will not be able to make claims for immaterial damages.[211] This position, however, makes little sense, since the inclusion of immaterial damages cannot be equated with the requirement to actually assert such. After all, even a natural person would be able to solely claim material damages where only those have been incurred and no other harm has come to the individual. More convincing is the position that that the protection of legal persons is not in the intent of the GDPR since Article 1, which outlines the subject matter and objectives, only mentions the rules relating to the protection of the fundamental rights of *"natural persons"*.[212] In that sense, it remains to be seen how courts decide to handle claims made by legal entities, if this was ever attempted. It does, however, at least seem possible for a legal person to try to enforce compensation under Art. 82, since the provision does not formally seem to exclude them. Some sources also refer to the definition of data subjects under Art. 4 No. 1, which also only includes natural persons.[213] This argument, however, only makes sense if it was to be assumed that only data subjects were to be eligible to demand damages under Art. 82.

---

[210] *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204; *Paal*, 1 MMR 2020, 14, 14; *Kohn*, 11 ZD 2019, 498, 502; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 13; Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 11; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 8.

[211] Taeger/Gabel / *Moos/Schefzig*, Art. 82 DS-GVO, para 17; Wybitul / *Krätschmer/Bausewein*, Art. 82 DSGVO, para 14.

[212] *Paal*, 1 MMR 2020, 14, 14; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 13; *Kohn*, 11 ZD 2019, 498, 502; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 8.

[213] *Paal*, 1 MMR 2020, 14, 14.

(2) Limitation to Data Subjects

The second point of contention concerns precisely that issue: whether or not natural persons, other than those to whom the information is relating, should be able to claim damages under Art. 82.[214] Proponents of limiting the right to compensation and liability to data subjects argue that both Art. 83(4) and Recital 146 only refer to the full and effective compensation of *"data subjects"*.[215] German courts also seem to be split on the issue, with some allowing claims by third parties[216] and others denying such a right.[217] Despite that, the prevailing opinion seems to be in support of allowing claims made by individuals other than the person to whom the processed data is relating if they have incurred damages due to the infringement as well.[218] This reading of the provision should also generally be followed, since incorrect processing of personal data can also lead to significant losses for other individuals, in particular where they are close to the data subject, either because of a working relationship (for example incorrect information about the creditworthiness of a partner of a partnership under civil law (GbR) will also affect the other partners)[219] or due to family ties.[220]

---

[214] *Kohn*, 11 ZD 2019, 498, 502; *Wybitul/Leibold*, 4 ZD 2022, 207, 210; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 113f; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 203-204; *Paal*, 1 MMR 2020, 14, 14f; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 9; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 15.

[215] *Wybitul/Leibold*, 4 ZD 2022, 207, 210.

[216] OLG Hamburg, ZD 2019, 33, para 36.

[217] BAG, ZD 2022, 56, para 33; LG Magdeburg, GRUR-RS 2019, 197, para 15.

[218] *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 9; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 15; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 113f; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 203-204; *Paal*, 1 MMR 2020, 14, 14f; *Geissler/Ströbel*, 47 NJW 2019, 3414, 3414.

[219] *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 9; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 15.

[220] *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 113f; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 203-204; *Kohn*, 11 ZD 2019, 498, 502; *Geissler/Ströbel*, 47 NJW 2019, 3414, 3414.

bb) Damages

First of all, Art. 82(1) provides that in order for a person to be able to make a claim for compensation, they must have suffered damages. These can be both of a material, as well as non-material nature. Recital 146 also provides in that context that the concept of damages is to be interpreted broadly in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of the GDPR. This clarification likely serves not only the purpose of assuring a high level of protection for data subjects, but also a uniform understanding of this term among Member States, who otherwise might be inclined to use national law as the basis for their interpretation, which could constitute a significant hindrance in the effective enforcement of this right.[221] It is also important to note that Art. 82 of the GDPR is directly applicable, meaning that individuals seeking compensation no longer need to rely on existing torts found in Member State law in order to enforce their claims.[222]

(1) Material Damages

Material damages will naturally be easier to assess but might on the other hand be rarer, since the right to privacy and protection of one's personal data are in themselves of a rather intangible nature. An issue might, however, occur as a result of the processing of incorrect information or through the deduction of incorrect inferences, for example, if an individual would be denied a credit or a purchase based on such.[223] Material damages could also occur as a result of having to initiate a legal action in order to avoid or mitigate immaterial damages, resulting from improper processing activities.[224]

---

[221] *Paal*, 1 MMR 2020, 14, 16; Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Keppeler/Jacquemain,* 'Art. 82' DSGVO, para 7.

[222] Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1175.

[223] Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 12; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 19.

[224] *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 114; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 28.

Questionable, however, is to what extent accidental or unlawful destructions, alteration, or disclosures towards third parties can be considered as such.[225] This might be relatively easy where transmitting information to the wrong recipient has caused a direct material loss.[226] Where, however, the financial disadvantage suffered by the individual lies rather in the loss of control over the data or the fact that they were unable to generate profit from the disclosure themselves, the demarcation becomes significantly harder[227] as it relates to the fundamental questions of the economic value of data.[228] While courts have so far not been inclined to accept the assertion of damages in such a form,[229] it does seem possible, especially in consideration of the "broad interpretation" required by the GDPR in that context.[230] It should, however, be noted that individuals would probably need to be able to evidence some form of opportunities for commercialisation, which they have theoretically lost, in order to make such a claim.[231]

(2) Immaterial Damages

The extent of the potential scenarios giving rise to immaterial damages will be significantly broader than was the case with material losses, since the right to data protection constitutes a personal right and will therefore be more susceptible to emotional injuries. While the Regulation does not give any specific examples as to the types

---

[225] *Paal*, 1 MMR 2020, 14, 16; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 19.

[226] For example, if credit card details were transmitted to the wrong recipient and that person went on to use the card for their own payments and could not be identified.

[227] *Paal*, 1 MMR 2020, 14, 16; *Strittmatter/Treiterer/Harnos*, 12 CR 2019, 789, 791-794.

[228] For more on that question see for example: *Wandtke*, 1 MMR 2017, 6, 6ff; *Schweitzer/Peitz*, 5 NJW 2018, 275, 275ff; *Hacker*, 2 ZfPW 2019 148, 148ff.

[229] See for example: OLG Dresden, ZD 2019, 567, para 13.

[230] *Strittmatter/Treiterer/Harnos*, 12 CR 2019, 789, 791; *Paal*, 1 MMR 2020, 14, 16; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 28.

[231] *Paal*, 1 MMR 2020, 14, 16; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 20.

of impairments that might occur, Recital 75 provides a quite comprehensive overview of potential risks to the rights of freedoms of data subjects which might occur as a result of infringements of the applicable law. Typical dangers individuals will therefore be exposed to include discrimination, identity theft or fraud, damage to reputation, loss of confidentiality of personal data, unauthorised reversal of pseudonymisation, and social disadvantages resulting from the lack of control over one's personal information.

Problematic as always with regards to the enforcement of highly personal rights is the question of calculating actual damages for such infringements. Recital 146 only specifies that the granted compensation would need to be *"full"* and *"effective"*. The criterion of effectiveness is already well established in the CJEU Case Law dealing with infringements of personal rights, in particular in the context of discrimination, and is commonly understood as requiring damages to be sufficiently high to have a deterring effect on the guilty party so that the purpose of the law can be adequately realised.[232] In consequence, additionally to the specific circumstances of the data subject, those of the controllers will also have to be taken into consideration in order to ensure that they are appropriately incentivised not to allow the occurrence of similar consequences in the future.[233] These considerations should, however, not be confused with the administration of punitive damages which in accordance with the Principle of Equivalence should only be awarded where national law would also allow

---

[232]Case 14/83 *Colson and Kamann* [1984] ECLI:EU:C:1984:153, para 23, 28; Case C-271/91 Marshall [1993] ECLI:EU:C:1993:335, para 24; Case C-180/95 Draehmpaehl [1997] ECLI:EU:C:1997:208, para 25; Case C-407/14 Arjona Camacho [2015] ECLI:EU:C:2015:831, para 31, 34.

[233] *Cordeiro*, 5 EDPL 2019, 492, 494; *Kohn*, 11 ZD 2019, 498 501; *Strittmatter/Treiterer/Harnos*, 12 CR 2019, 789, 794; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 115; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 206; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 18d.

for this type of penalisation under similar circumstances.[234] It is, however, commonly accepted that courts should take account of the criteria outlined in Art. 83(2) used for the determination of administrative fines when deciding on the specific value of the "full and effective" compensation to be awarded to the data subject.[235] Included therein are elements such as: the nature, gravity, and duration of the infringement; its intentional or negligent character; actions taken in order to mitigate potential damages; the degree of responsibility; previously caused infringements; the degree of cooperation with the supervisory authority; categories of personal data; and the number of data subjects affected, as well as the nature, scope, and purpose of the initial processing activity.

cc) Infringement of the Regulation

Art. 82(2) requires the existence of an infringement of the Regulation in order for a claim against the controller to materialise. As has been outlined in Part 2 Chapter 3: A. VI. 1. Responsibility previously, the data controllers take a central role when it comes to the responsibility for the processing of personal data under the GDPR. In that sense, the Regulation assigns them with numerous obligations directed towards the assurance of secure processing of personal data, while additionally requiring them to be able to demonstrate their compliance at any given time. Should any of these obligations not be fulfilled, an infringement of the regulation can be concluded.[236] Incompliance with other laws will, however, not be considered as a

---

[234]Joined cases C-295/04 to C-298/04 Vincenzo Manfredi and Others [2006] ECLI:EU:C:2006:461, para 93; *Cordeiro*, 5 EDPL 2019, 492, 494; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 206.

[235]*Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 206; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 18d; *Paal*, 1 MMR 2020, 14, 17; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 115.

[236]Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Keppeler/Jacquemain,* 'Art. 82' DSGVO, para 86; *Paal*, 1 MMR 2020, 14, 15; *Kohn*, 11 ZD 2019, 498, 499f.

sufficient ground for a claim under Art. 82.[237] Infringements of delegation and implementation acts adopted in accordance with the GDPR and Member State law specifying the Regulation will, on the other hand, also fall under that claim, according to Recital 146.

dd) Causation

Additionally, to the materialisation of damages on the side of an individual and the existence of an infringement on the side of the data controller, the Regulation also requires the establishment of a causal link between the two.[238] This is evidenced by the wording used both in Art. 82(1) (*"as a result of"*) and (*"caused by"*). In accordance with the prevailing opinion, these terms should also be interpreted in accordance with the case law of the Court of Justice, in consideration of the objectives of the Regulation.[239] In particular, experiences from the field of competition and antitrust law seem to be suitable for applying here as well, as under both damages are subject to the Principle of Equivalence and have been established as fulfilling a deterring and not just purely compensatory function.[240]

While the CJEU typically requires that damages constitute a *"sufficiently direct consequence"* of the infringement,[241] the requirements in the context of civil liability for violations of EU competition rules are slightly lower, with the court only demanding a *"causal relationship"*

---

[237]Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 20.

[238]Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1175; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 41; Paal/Pauly / *Frenzel*, Art. 82 DSGVO, para 11; *Cordeiro*, 5 EDPL 2019, 492, 495.

[239]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 41; Paal/Pauly / *Frenzel*, Art. 82 DSGVO, para 11; *Paal*, 1 MMR 2020, 14, 17; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 115f.

[240]*Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 115f; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 41; Paal/Pauly / *Frenzel*, Art. 82 DSGVO, para 11; *Paal*, 1 MMR 2020, 14, 17 *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 206.

[241]Joined cases 64 and 113/76, 167 and 239/78, 27, 28 and 45/79 *P. Dumortier frères SA and others* [1979] ECLI:EU:C:1979:223, para 21; Case C-199/11 *Europese Gemeenschap* [2012] ECLI:EU:C:2012:684, para 65.

between the harm and the prohibited practice.[242] The specifics of this term are left to the interpretation of the Member States, taking into account the principle of effectiveness enshrined in Art. 4(3) TEU.[243] National notions of causality which are too narrow will therefore not be applied.[244] This might, for example, be relevant where Member State Law requires a certain level of predictability of the harm by the injuring party, since the CJEU only refers to aspects and circumstances which *"could not be ignored"* by such.[245] While some sources consider the transferability of these rules onto the determination of damages under the GDPR as potentially going too far,[246] a significant rise in the proceedings regarding such, the total of cases where damages are awarded, as well as the actual amounts, seems inevitable.[247]

ee) Burden of Proof

In principle, the rules regarding the burden of proof would require for the claimant to evidence the presence of the above-mentioned criteria, namely the existence of damages and an infringement of the

---

[242]Joined cases C-295/04 to C-298/04 *Vincenzo Manfredi and Others* [2006] ECLI:EU:C:2006:461, para 61; Case C-199/11 *Europese Gemeenschap* [2012 Case C-199/11 *Europese Gemeenschap* [2012] ECLI:EU:C:2012:684] ECLI:EU:C:2012:684, para 43; Case C-557/12 *Kone AG and Others* [2014] ECLI:EU:C:2014:45, para 22.

[243]Case C-557/12 *Kone AG and Others* [2014] ECLI:EU:C:2014:45, para 32.

[244]*Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 116; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 45.

[245]Case C-557/12 *Kone AG and Others* [2014] ECLI:EU:C:2014:45, para 34.

[246]Paal/Pauly / *Frenzel*, Art. 82 DSGVO, para 11; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 206.

[247]*Wybitul/Leibold*, 4 ZD 2022, 207, 207; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 115; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 207; *Kohn*, 11 ZD 2019, 498, 502.

Regulation on the side of the controller, as well as a causal link between the two.[248] This is also generally applied under the Data Protection Directive.[249] Arguably, though, the GDPR might have caused a shift in that regard through the introduction of the principle of accountability.[250] In accordance with Art. 5(2), it is the responsibility of the controller to be able to demonstrate compliance with the Regulation. Similar obligations of being able to prove the adherence to the law are also found in other Articles of the GDPR, for example Art. 7(1) (*"the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data"*); Art. 11 (2) (*"the controller is able to demonstrate that it is not in a position to identify the data subject"*); Art. 12(5) (*"[t]he controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request"*) or Art. 24(1) (*"be able to demonstrate that processing is performed in accordance with this Regulation"*). Based on that, some sources conclude that the burden of proof should be reversed for claims of damages under Art. 82,[251] whereas others argue that such a reversal would cause significant procedural risks and could therefore not have been intended by the lawmakers.[252]

Looking at the wording used in Art. 82, it seems unlikely that there was an underlying intention to shift the burden of proof completely onto the data controller. After all, Paragraph 3 does introduce an obligation for such to prove that they are not responsible for the event, if they wish to be exempt from liability. Since such a stipulation is not contained anywhere else in the Article, it should be assumed that the generally accepted procedural rules should apply in that regard.

---

[248]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 46; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 116; *Paal*, 1 MMR 2020, 14, 17.

[249]*Van Alsenoy*, 7 JIPITEC 2016, 271, 274-276.

[250]*Wessels*, 43 DuD 2019, 781, 782; *Paal*, 1 MMR 2020, 14, 17; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 203; *Kohn*, 11 ZD 2019, 498, 502.

[251]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 46; *Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Paal*, 1 MMR 2020, 14, 17.

[252]*Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 203; *Wybitul/Leibold*, 4 ZD 2022, 207, 209.

Courts have also generally not been inclined to accept such a principal shift of the burden of proof and have largely relied on the commonly applicable rules in that regard.[253] This, however, should not mean that the principle of accountability has no practical effect in that context. Rather, it can be concluded that while the claimant will have to evidence the fact that they have incurred damages which resulted from the conduct of the controller, the business will be required to openly demonstrate the specifics of the internal processing procedures.[254] In that sense, the legal burden of proof remains with the injured party, whereas the duty to provide evidence is de facto shifted onto the defendant.[255]

Clarifications with regard to the burden of proof under Art. 82 have also recently been provided by the CJEU in the context of the ruling on *VB v. Natsionalna agentsia za prihodite.*[256] Here the Court clearly stated that *"the controller in question bears the burden of proving that the security measures implemented by it are appropriate".*[257] This would support the above understanding, that while the claimant still needs to evidence the causation of damages, once such damages have been assessed, it is for the controller to prove that there has been no violation of the GDPR on their side.

ff) Exemption

Even where an infringement of the Regulation has caused a person to suffer material or non-material damages, controllers might be

---

[253]LG Frankfurt/M., ZD 2021, 653, para 27f; LG Frankfurt/M., ZD 2020, 639, para 43; OLG Dresden, ZD 2022, 159, para 12; AG Frankfurt/M., ZD 2021, 47, para 32; LG Hamburg, ZD 2021, 99, para 29; OLG Brandenburg, ZD 2021, 693, para 4.

[254]*Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Kohn*, 11 ZD 2019, 498, 502; *Van Alsenoy*, 7 JIPITEC 2016, 271, 283.

[254]*Van Alsenoy*, 7 JIPITEC 2016, 271, 283.

[255]*Van Alsenoy*, 7 JIPITEC 2016, 271, 283.

[256]Case C-340/21 *VB v. Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986

[257]Case C-340/21 *VB v. Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986, para 57.

exempted from liability in accordance with Art. 83(3) if they are able to prove that they are *"not in any way responsible for the event giving rise to the damage"*. Since the applicability of Paragraph 2 would already imply the presence of an infringement, the entity in question would therefore have to argue that they cannot be held accountable for such. Unfortunately, the GDPR does not provide any explicit examples as to when this might be the case. Interestingly, the Data Protection Directive, which also allowed for the exemption from liability for controllers where they prove not to be responsible for the event which caused the damage under Art. 23(2), did provide further details in Recital 55, establishing that this applies *"in particular in cases where he establishes fault on the part of the data subject or in case of force majeure"*. Although the GDPR lacks such a clarification, these two instances should however still be assumed as giving rise to an exculpation under Art. 82(3) as well.[258] Businesses might be freed from accountability to include scenarios where they are not to be considered as a controller for the processing activity in question,[259] or where they are able to evidence the lack of a causal link between their misconduct and the damages.[260]

When comparing the wording under Art. 23(2) of the DPD and Art. 82(3) of the GDPR, it also seems that there was an intention to limit the scenarios for exculpation on the side of the lawmakers.[261] While controllers previously only needed to prove that they were not responsible, the Regulation now requires them to evidence that they are *"not in any way"* responsible. This means that even the slightest level of negligence on the side of the controller will exclude the possibility of exemption under Art. 82(3).[262] Businesses will also be fully

---

[258]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 54; *Paal*, 1 MMR 2020, 14, 17; *Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Van Alsenoy*, 7 JIPITEC 2016, 271, 283.

[259]Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1176.

[260]Ehmann/Selmayr / *Nemitz*, Art. 82, para 52.

[261]*Larouche/Peitz/Purtova*, CERRE Policy Report, 58; *Van Alsenoy*, 7 JIPITEC 2016, 271, 283.

[262]Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Keppeler/Jacquemain,* 'Art. 82' DSGVO, para 33; Kühling/Buchner / *Bergt*, Art. 82

liable for the (mis)conduct of their employees, regardless whether or not these were acting in accordance with internal policies or instructions of their supervisor.[263] This also includes potentially incorrect or inaccurate advice provided by the Data Protection Officer.[264] In accordance with Art. 39, the DPO predominantly fulfils advisory and auditing tasks, therefore the responsibility for assuring compliance with the Regulation cannot be shifted towards them, especially since they constitute a part of the entity which designates them.[265]

Highly debated in that context is, however, the extent to which controllers can exculpate themselves from liability where damages were caused by the misconduct of a processor acting against received instructions. On the one hand, where such vendors are being sufficiently supervised, it can be argued that a business is in no way responsible for their wrongdoing.[266] This would create the burden of evidencing such seamless supervision on the side of the controller which can be regarded as almost impossible, considering the amount of outsourcing agreements a typical enterprise will have in place.[267] Regardless of practical implications for the controller, allowing exculpation based on the controller's fault would bode significant consequences for the injured individual. As a result, they would be forced to redirect the claim against such a processor or sub-processor. This could, after all, seriously hinder the receipt of appropriate compensations where, for example, such a processor constitutes a smaller

---

DSGVO, para 54 *Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Paal*, 1 MMR 2020, 14, 17; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204.

[263]Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 25; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 55; Ehmann/Selmayr / *Nemitz*, Art. 82, para 53; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 116; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204; *Paal*, 1 MMR 2020, 14, 17.

[264]Ehmann/Selmayr / *Nemitz*, Art. 82, para 53; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 55a; *Wybitul/Leibold*, 4 ZD 2022, 207, 210.

[265]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 55a.

[266]Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 25; Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1176.

[267]*Paal*, 1 MMR 2020, 14, 17.

entity or is confronted with insolvency issues.[268] It would also pose a potential impediment if the responsible party was located in a different or even third country. Such a result would simply be unacceptable in the consideration of the established purpose of assuring effective compensation (Art. 82(4)).[269] Such an interpretation would also go against the general intent of the GDPR which explicitly constructs the controllers as the entity which has to hold the responsibility vis-a-vis the data subject, and Paragraph 4, which stipulates that the involved parties are to be held liable for the entirety of the damages, rather than just their respective parts.[270] The result in which the controller has to be liable towards the injured party for damages caused by a processor can also not be considered unfair, since such an entity will, after all, still be able to claim the awarded compensation back from their vendor in accordance with Art. 82(5).[271]

VII. Interim Conclusions: Controller

The definition of "controller" can be found in Art. 4 No. 7 of the GDPR, where this party is defined as the natural or legal person, public authority, agency, or other body which alone or jointly with others, determines the purposes and means of the processing of personal data. There are, therefore, no formal restrictions as to the type of entity or person which could take that role, as long as they are in fact determining the means and purposes of the processing of personal data. The element of "determination", which requires real control over the activities at hand, can stem from both legal designation (either in an explicit or implicit form) or from the actual factual influence the party holds. It is considered largely irrelevant what entity is physically conducting the processing, as the question

---

[268] *Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Paal*, 1 MMR 2020, 14, 18; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 55.

[269] *Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Paal*, 1 MMR 2020, 14, 18; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 55.

[270] Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 55; *Wybitul/Haß/Albrecht*, 3 NJW 2018, 113, 114.

[271] For more details see Part 2 Chapter 3: B. III. 2. b) Liability.

of authority over the process is to be considered the decisive element.

This authority needs to be exercised with regards to two elements: the means and the purposes of the processing activity, also commonly referred to as the “why” and “how” of data processing, meaning the controller should determine why personal data is being processed in the first place and how this should be done. In constellations involving multiple entities having an effect on the processing activities in question, the question arises as to which extent influence might be exerted by a party without being considered a controller. The general consensus in that regard supports the idea that the decisive element for attaining controller status is the determination of purposes, whereas decisions with regards to the means can also, to a certain extent, be taken by processors. In order to specify the extent of the processors’ margin of manoeuvre, a division into “essential” and “non-essential” means is suggested, where decisions about the first are still to be reserved to the controller; the latter on the other hand, are free to be left to the processor.

It is also important to note that the determination regarding the means and purposes needs to be concerned with the processing of personal data, and not any other elements in order to be relevant for the establishment of the parties’ respective roles. For example, in instances where such processing only constitutes a subsidiary effect to the overall relationship between the parties, it cannot be assumed that the controllership lies with the “stronger” counterpart or with the entity outsourcing a certain service. Rather, the actual influence over the processing activity needs to be asserted.

The controller basically takes the central role when it comes to the responsibility for the processing of personal data under their control, as it is their obligation to assure the compliance of such with the GDPR, while additionally having to be able to demonstrate this at any given time. The consequences of incompliance with the provisions of the GDPR can be broadly put into two categories: measures imposed by the data protection authorities or direct liability for suffered damages towards individuals.

Supervisory authorities are given a number of competences in order to enforce the Regulation; these are referred to as “powers” under Art. 58 and have been divided into three categories: investigative powers, corrective powers, and authorisation and advisory powers. Investigative powers serve the purpose of allowing supervisory authorities to establish the relevant facts surrounding the processing of personal data. Authorisation and advisory powers allow the DPA to support all relevant actors in assuring an appropriate level of protection for the processing of personal data in accordance with the requirements of the Regulation. Most relevant in the context of potential consequences incurred by controllers are the corrective powers, which aim to enforce the rectification of potential infringements of the law. This can be done in the form of warning and reprimands, orders, legal proceedings, and fines.

In addition to the sanctions a controller can receive from the supervisory authorities, they may also be liable for any material or non-material damages incurred by a person as a result of an infringement of the regulation caused by them. The elements which need to be present for such a claim to arise are: the occurrence of damages on the side of the party making the claim, an infringement of the Regulation by the controller, and a causal link between the two. While it cannot be assumed that the GDPR allows for a reversal of the burden of proof, the demonstration of the relevant elements is in a sense simplified for the claimant, due to the principle of accountability. It is therefore generally considered that the legal burden of proof remains with the injured party, whereas the duty to provide evidence is de facto shifted onto the defendant. Controllers can, however, be exempted from liability if they are able to prove that they are in no way responsible for the event giving rise to the damages.

Based on all of these factors, it can be concluded that the controller is the central figure when it comes both to decision-making with regards to the processing of personal data, as well as the responsibilities resulting from this authority.

B. Proccessor

As per Article 4 No. 8 of the GDPR, processors are defined as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*.

I. Personal Element

General considerations with regards to this aspect have already been outlined above and since the scope of bodies listed under the definition is exactly the same as under Art. 4 No. 7, we can largely refer to the considerations and conclusions outlined therein.[272] There are, however, aspects which differentiate the personal element in the context of commissioned data processing which need to be considered.

1. Seperate Legal Entity

First of all, the processor needs to be a separate legal entity from the controller.[273] This means that within a global undertaking, separate legal entities can be processors and controllers with regard to each other as the GDPR does not recognise an intra-group-privilege.[274] Actions of employees, the workers' council, or specific departments within a legal undertaking are, however, still to be attributed directly to the controller.[275]

2. Providing Guarantees

Article 28(1) also provides that where a controller wishes to outsource a processing activity to another entity, assurances must be given that such a processor is able to provide *"sufficient*

---

[272]See Part 1 Chapter 1: A. I. Personal Element.

[273]*EDPB*, Guidelines 07/2020, para 74f; Kühling/Buchner / *Hartung*, Art. 4 Nr. 8 DSGVO, para 6; Kuner and others / *Bygrave/Tosoni*, Art. 4(8), 157, 159.

[274]*Voigt/von dem Bussche*, GDPR, 18.

[275]Kühling/Buchner / *Hartung*, Art. 4 Nr. 8 DSGVO, para 6; *EDPB*, Guidelines 07/2020, para 75; *Jung/Hansch*, 4 ZD 2019, 143, 146-148.

guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". In turn, service providers who are unable to provide such guarantees shall not be deployed. This means that due diligence is required from the controller when selecting vendors, to which the processing of personal data might potentially be outsourced.[276]

Recital 81 further specifies that these can especially concern aspects such as the level of expert knowledge demonstrated by a vendor, as well as their reliability and resources available for them in the implementation of appropriate technical and organisational measures. A focus on the assurance of these means is, after all, logical especially since processors are *often* given a quite large margin of discretion in determining the details of these aspects.[277] Article 28(5) also provides that additional factors which may also be taken into account when assessing the suitability of a certain processor are their adherence to an approved code of conduct or certification mechanism in accordance with Articles 40 and 42, respectively. In consideration of the principle of accountability (Art. 5(2)) it is also safe to assume that this requirement of due diligence when selecting a potential contractor also encompasses a requirement to properly document such a verification procedure.[278]

II. Substantive Element

The fundamental component of the designation as a processor, however, lies in the factor that the *processing of personal data* is being performed *on behalf of* another legal entity.

---

[276] *Petri*, 7 ZD 2015, 305, 308f; Sydow/Marsch / *Ingold*, Art. 28, para 32; *Kühling*, in: Datenschutzrecht, para 560.

[277] See Part 1 Chapter 1: B. II. 2. b) Margin of Discretion.

[278] *Gürtler*, 2 ZD 2019, 51, 53; *Kühling*, in: Datenschutzrecht, para 560; Sydow/Marsch / *Ingold*, Art. 28, para 33.

1. Processing of Personal Data

Both the relevance and the actual content of this characteristic have also already been outlined in the context of the definition of data controller (see Part 1 Chapter 1: A. II. 3. Processing and 4. Personal Data). It is, however, important to remember that all considerations with regards to the relationship between two parties, in the context of the processing of personal data, should solely focus on that element. While the idea of the functionality of the concepts of controller and processor under the GDPR asks for the specific circumstances of the case to be considered, this does not refer to elements outside of the scope of the processing operations, unless they have a direct effect on such.

Even though a specific entity might therefore be paying for a service, using a subsidiary, putting forward instructions, or using a contractor, this will not automatically result in a controller-processor relationship unless the relevant service, instructions, or contract concerns the processing of personal data. For example, where a company is being engaged for purposes such as facility management, the transport of goods, consultancy or furnishing, they will naturally act “on behalf“ of their customer but this will not entail a processing of personal data for such. Here, the nature of the provided service is rooted in a completely different activity and while personal data might be processed as a by-product of the underlying relationship, for example, in the form of contact details for communication purposes, bank account information for payment purposes, or an address for delivery, the essence of the relationship does not relate to the processing of personal data.[279] Any processing will also not be conducted “on behalf of” another entity as in these instances, the customer will not be giving any instructions to their contractor, with regard to such.[280] The EDPB does note, however, that even where the processing of personal data does not constitute the primary object of the service, an entity might still be considered as a processor,

---

[279] *Seiter*, 43 DuD 2019, 127, 129; *EDPB*, Guidelines 07/2020, para 80.
[280] Kuner and others / *Bygrave/Tosoni*, Art. 4(8), 157, 160.

should the means and purposes still be determined by the customer.[281]

2. On Behalf of the Controller

The determination of the element of processing personal data *on behalf of* the controller is the one typically causing the largest amount of practical challenges when attempting to assess a specific relationship between entities at hand.[282] This can largely be attributed to the fact that business relationships tend to be rather complex and do not necessarily follow strict standards or delineations.[283] While in that sense, the intent of treating these terms as a functional and autonomous concept was likely rooted in the idea of having them adapt to the changing conditions of the market, in the interest of technological neutrality this naturally also leads to a large amount of legal uncertainty on the side of businesses.[284] All relevant aspects of this characteristic should therefore be carefully examined below.

a) Instructions

In principle, the relationship between the controller and the processor has been constructed as one of subservience in which the processor should be acting in accordance with the controller's demands and directions.[285] This results directly from the prerequisites of such a relationship outlined in Art. 28, as Paragraph (3)(a) therein provides that any contract or legal act governing such should stipu-

---

[281] *EDPB*, Guidelines 07/2020, para 81.

[282] Eßer/Kramer/von Lewinski / *Kramer*, Art. 28 DSGVO, para 8ff.

[283] *Lindqvist*, 26 Int. J. Law Inf. Technol. 2018, 45, 50.

[284] https://medium.com/databulls/is-europes-data-protection-regulation-gdpr-on-the-verge-of-collapse-844a2fa7dd6 (accessed 16 October 2024); https://www.datenschutz-notizen.de/kein-auftragsverarbeitungsvertrag-mehr-fuer-videokonferenz-tools-0237051/ (accessed: 26 February 2026); https://www.datenschutz-notizen.de/who-is-the-controller-for-data-processing-and-who-is-the-processor-2727529/ (accessed: 26 February 2026).

[285] Kuner and others / *Bygrave/Tosoni*, Art. 4(8), 157, 160.

late that the processor has to process personal data *"only on documented instructions from the controller"*. Any entity processing personal data "on behalf of" another will therefore need to be bound by their instructions.[286] The obligation to document these has been newly introduced by the GDPR as it was not contained in the wording under the Data Protection Directive.[287] Its intent should, however, be considered as being in line with the principle of accountability enshrined in Art. 5(2).[288] Since the Regulation does not define a specific form which would need to be adhered to, controllers should not be precluded from ordering certain activities orally, as long as the proper form of documentation is assured.[289] It is, however, generally advisable for the parties to agree in advance on the proper form of transmission and documentation of such.[290]

Also related to the provision of instructions by the controller are the stipulations outlined in points (g) and (h) of Art. 28, which introduce obligations of the processor to delete or return data and to make available all information which might be necessary in order to demonstrate compliance with the Regulation, where ordered to do so by the controller. Additionally, Art. 28(2) specifies that a processor requires the specific written authorisation from the controller in cases when they wish to engage any sub-processors.

This general requirement to follow instructions given by the controller is further expedited by Article 29, which stipulates such an obligation for the processor, as well as all individuals acting under the authority of a controller or processor; the only exemption is applied

---

[286]*Nickel*, 3 ZD 2021, 140, 141f; *Folkerts*, ZD 2022, 201, 202; *Lezzi/Oberlin*, 9 ZD 2018, 398, 399.

[287]*Müthlein*, 2 RDV 2016, 74, 76; *Petri*, 7 ZD 2015, 305, 309; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 66.

[288]Eßer/Kramer/von Lewinski / *Kramer*, Art. 28 DSGVO, para 50.

[289]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 99; Eßer/Kramer/von Lewinski / *Kramer*, Art. 28 DSGVO, para 50; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 29' DSGVO, para 103; Ehmann/Selmayr / *Bertermann*, Art. 28, para 24.

[290]Ehmann/Selmayr / *Bertermann*, Art. 28, para 24; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 29' DSGVO, para 103.

where there is a conflicting requirement enshrined in Union or Member State law. While this can arguably be considered as somewhat redundant as the same would already follow from Art. 28(3)(a),[291] the provisions were likely kept in order to reiterate the fact that confidentiality and security obligations extend to the employees of each entity as well.[292] Furthermore, it serves the purpose of reinforcing the idea of the processors' obligation to conform with a controller's instructions as the central element of commissioned data processing.[293]

The importance of following these instructions for the characterisation as a processor is further underlined by Art. 28(10), which provides that in instances where an entity contractually designated as a processor infringes the provisions of the GDPR through determining the means and purposes of processing on their own, they shall be considered as a controller with regard to that processing activity. This again not only emphasises the functional character of these concepts but also accentuates how crucial it is for the processor to actually follow the instructions given by their customer, as otherwise they will effectively hold all legal responsibility assigned to a controller under the GDPR.[294]

b) Margin of Discretion

While the adherence to the controllers' instructions constitutes a central prerequisite for the characterisation as a data processor in the meaning of Art. 4 No. 8 GDPR, there is also a general consensus

---

[291]Eßer/Kramer/von Lewinski / *Kramer*, Art. 29 DSGVO, para 1; Kuner and others / *Millard/Kamarinou*, Art. 29, 612, 614f; Kühling/Buchner / *Hartung*, Art. 29 DSGVO, para 2.

[292]Eßer/Kramer/von Lewinski / *Kramer*, Art. 29 DSGVO, para 2; Kuner and others / *Millard/Kamarinou*, Art. 29, 612, 615.

[293]Kuner and others / *Millard/Kamarinou*, Art. 29, 612, 613; Ehmann/Selmayr / *Bertermann*, Art. 29, para 4.

[294]Eßer/Kramer/von Lewinski / *Kramer*, Art. 28 DSGVO, para 55; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 29' DSGVO, para 171; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 103; *EDPB*, Guidelines 07/2020, para 79.

that it is still possible to leave processors with a certain amount of discretion regarding the specific execution of the commissioned processing operations.[295] This raises the question of how wide the margin of manoeuvre granted to a processor can be before the entity needs to be functionally considered as a controller.[296] Since a controller, as per definition, constitutes a natural or legal person determining the means and purposes of the processing activity, all decisions made by a vendor outside of these two aspects will logically not have any legal effect on the designation of their role under the GDPR. Regarding the relevant aspects of the "how" and "why" of the processing of personal data, it is generally considered that the purposes should solely be defined by the controller.[297] This is, after all, logical, as the controller is also the one obliged to assure the existence of a valid legal basis for the processing operation. Additionally, any personal interest of an entity in a certain activity, beyond simply fulfilling a contractual service obligation, will naturally go beyond the scope of "acting on behalf" of the customer.[298]

It is, on the other hand, commonly accepted that the processor can be granted with a certain margin of discretion when it comes to the selection of the means of the processing of personal data, within a certain outsourced assignment.[299] The Art. 29 WP introduces in that context the concept of "essential means" which are solely to be

---

[295] *EDPB*, Guidelines 07/2020, para 78; Rücker/Kugler, *Rücker*, B. Scope of application, para 136ff; Kühling/Buchner / *Hartung*, Art. 4 Nr. 8 DSGVO, para 7; *Hartung/Büttgen*, 41 DuD 2017, 549, 550.

[296] Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13; *EDPB*, Guidelines 07/2020, para 35; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 150; *Monreal*, 12 ZD 2014, 611, 612.

[297] Rücker/Kugler, *Rücker*, B. Scope of application, para 134; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13; *EDPB*, Guidelines 07/2020, para 37 *Art. 29 WP*, Opinion 1/2010, 15; Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Mühlenbeck,* 'Art. 4' DSGVO, para 122.

[298] *Sury*, 44 Informatik Spektrum 2021, 376, 376.

[299] *Kühling*, in: Datenschutzrecht, para 551; Kuner and others / *Bygrave/Tosoni*, Art. 4(8), 157, 160; *EDPB*, Guidelines 07/2020, para 35; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 37.

determined by the processor and other less crucial elements, which can be decided upon by the processor.[300] This division into "essential" and "non-essential" has since then also been supported by the EDPB and applied by numerous other sources.[301] Elements typically categorised as "essential" include the type of personal data being processed, the effect on data subjects, the duration of the processing, and the potential recipients.[302] Such an understanding would also be supported by Art. 28(3) since these are also the elements which need to be determined through a legal act governing the processing. Traditionally defined as "non-essential", on the other hand, are purely ancillary questions such as the choice of a specific hard- or software, selections of fonts, colours, or decisions on which employees to assign certain tasks.[303] A large amount of discretion is also commonly recognised in the selection of specific technical and organisational measures, especially where the controller might be relying on the expertise of the processor in that regard.[304]

c) Indicators of Delimination

This margin of discretion does, however, also often naturally lead to practical difficulties in differencing between the two, especially

---

[300]*Art. 29 WP*, Opinion 1/2010, 14: "Against this background, while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means. In this perspective, it is well possible that the technical and organizational means are determined exclusively by the data processor".

[301]Rücker/Kugler, *Rücker*, B. Scope of application, para 135f; *EDPB*, Guidelines 07/2020, para 38; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 38; Kuner and others / *Bygrave/Tosoni*, Art. 4(8), 157, 160.

[302]Rücker/Kugler, *Rücker*, B. Scope of application, para 136ff; *EDPB*, Guidelines 07/2020, para 38; Kuner and others / *Bygrave/Tosoni*, Art. 4(8), 157, 160.

[303]Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 38; *EDPB*, Guidelines 07/2020, para 38; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 38.

[304]Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 37f; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 38.

when the decision-making power left to a certain contractor is in fact quite wide.[305] In that sense, both literature and Data Protection Authorities have suggested the use of certain indicators which can be used while attempting to make an accurate determination regarding the roles and responsibilities of the parties involved in the processing of personal data. Examples include questions such as: which entity decided to collect personal data in the first place,[306] who has the legal basis for doing so,[307] what types of data subjects are being targeted and what is their relationship with the vendor,[308] how detailed are the instructions given to the contractor,[309] to what extent is the provision of the service is being supervised or monitored,[310] or whether the service provider has particular expert knowledge in the field.[311]

Some sources also attempt to add some clarity by including specific examples of outsourcings typically considered as commissioned data processing. Listed in that context are for example payroll accounting,[312] cloud computing, letter shops, mail delivery, data-scanning or conversion, market research, and multiple types of IT services including hosting, maintenance, back-ups, and archiving.[313] Traditionally excluded from being considered a controller–processor

---

[305]*Kühling*, in: Datenschutzrecht, para 551; Gola/Heckmann / *Klug*, Art. 28 DSGVO, para 5; *Jung/Hansch*, 4 ZD 2019, 143, 147-148.

[306]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 28.

[307]*DSK,* Kurzpapier Nr. 13, 2; *EDPB*, Guidelines 07/2020, para 167.

[308]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 46; *CNIL*, GDPR, 3.

[309]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 46; *CNIL*, GDPR, 3.

[310]*Gündel*, 12 ZWE 2018, 429, 431; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 46; *CNIL*, GDPR, 3.

[311]*Ziegenhorn/Fokken*, 5 ZD 2019, 194, 197; *CNIL*, GDPR, 3; Gola/Heckmann / *Klug*, Art. 28 DSGVO, para 5; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 47.

[312]For more details on the legal classification of payroll administration refer to: *Kramer/Schmidt*, 4 ZD 2020, 194, 194 ff.

[313]*DSK,* Kurzpapier Nr. 13, 4; *CNIL*, GDPR, 2; Sydow/Marsch / *Ingold*, Art. 28, para 18-23.

relationship are, on the other hand, pure mail delivery or transportation services, freelancers such as trainers and consultants,[314] as well as occupations subject to professional secrecy such as lawyers, tax advisors, or medical professionals.[315] Due to the functional character of these concepts, the provided examples can, however, only be used in order to outline general tendencies but are not legally binding.

Another element which might be considered when assessing the overall relationship between two entities with regards to the processing of personal data is the presence of other elements listed in Art. 28. Art. 28(3), which includes a number of different stipulations not necessarily referring to the instructions provided by the controller but to the general content of the relationship, as well as the responsibilities on the side of the processor, such as the need to ensure confidentiality from individuals authorised to process personal data (point (b)); the assurance of the security of the processing operations in accordance with Art. 32 (point (c)); and the assistance of the controller in all of their obligations outlined in Articles 31-36 (point (d)). Where such responsibilities are agreed upon and adhered to by a contractor, this might generally serve as another indication for the presence of a controller–processor relationship, especially if some of the above-mentioned factors are present as well.

III. Effect

There are a number of legal stipulations which result from being considered a processor in accordance with Art. 4 No. 8 GDPR. Since these will also be relevant for providers of Personal Information Management Systems where they have been designated as such, the potential consequences of this qualification should be outlined below.

---

[314]For more details on the subject of the classification of freelancing refer to: *Conrad*, 43 DuD 2019, 134, 134ff.

[315]*DSK,* Kurzpapier Nr. 13, 4f; Gola/Heckmann / *Klug*, Art. 28 DSGVO, para 5; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 5.

1. Responsibilities

Where a processor is being engaged for the performance of a processing activity or part of such by the controller, certain legal obligations arise for the parties involved. Most importantly, the relationship between the parties needs to be governed by contract or legal act. Additionally, the GDPR imposes a number of direct obligations upon processors, all of which shall be discussed below.

a) Contract or other Legal Act

In accordance with Art. 28(3), any processing of personal data that is being conducted by a processor has to be governed by a contract or other legal act under EU or Member State law. In practice, the governance by contract is far more prevalent than the designation as a processor via a formal legal act.[316] Under the present legal situation, this form of governance will also generally apply for Personal Information Management Systems, as no legal act designating the roles of such currently exists. In that sense, the focus of the following section will also mainly relate to considerations with regards to the necessary contractual provisions. Since, however, both the formal and contextual requirements stipulated for these two governance forms are essentially the same, these considerations would largely apply for any potential legal acts as well.[317]

aa) Form

Article 28(9) stipulates that the *"contract or the other legal act referred to in Paragraphs 3 and 4 shall be in writing, including in electronic form"*. The requirement for a written or electronic format is, however, not to be equated with the legal definitions applicable to

---

[316] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO, para 49; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 62.

[317] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO, para 47.

those terms under Member State law.[318] The terminology is rather subject to an autonomous interpretation in accordance with EU data protection law.[319] It can therefore be assumed that any sort of designation of the respective roles and responsibilities of the parties put in writing would suffice as a data processing agreement under Art. 28(3).[320] In that sense, even forms such as scans of a signed contract or exchanging a contract via e-mail by using a simple digital signature would meet the formal requirements in that context.[321] In consideration of the lack of any other formal stipulations, it is also generally acceptable to include the provisions agreed upon between the parties with regards to the processing of personal data into a larger contract such as a Service Level Agreement or a Framework Service Agreement.[322]

bb) Content

Whereas the GDPR provides quite general formal requirements for the form in which agreements on commissioned data processing are to be concluded, Art. 28(3) introduces very specific stipulations in regard to the content of a contract or other legal act regulating such. It provides that it should set out elements such as the categories of personal data being processed, the affected data subjects, the subject-matter and duration of the processing, as well as its nature and purpose and the rights and obligations of the controller.

---

[318] *Kühling*, in: Datenschutzrecht, para 534; *Hartung/Büttgen*, 41 DuD 2017, 549, 554; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO, para 92.

[319] *Hartung/Büttgen*, 41 DuD 2017, 549, 554; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO, para 92; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 165.

[320] Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 165.

[321] *Kühling*, in: Datenschutzrecht, para 534; Eßer/Kramer/von Lewinski / *Kramer*, Art. 28 DSGVO, para 41.

[322] Kuner and others / *Millard/Kamarinou*, Art. 28, 599, 606; Eßer/Kramer/von Lewinski / *Kramer*, Art. 28 DSGVO, para 43.

The article subsequently outlines very specific conditions for any Data Processing Agreement, stating that it needs to stipulate that: (a) personal data is only processed based on the documented instructions of the controller, including any transfers to third countries or international organisations; (b) individuals processing personal data under the authority of the processor have been committed to confidentiality by such or are under an appropriate statutory obligation in that regards; (c) appropriate technical and organisational measures assuring the security of processing in accordance with Art. 32 GDPR are being taken; (d) sub-processors are only to be engaged where the controller has previously provided a specific or general written authorisation, and any intended changes with regards to such are communicated towards the controller in advance, giving such the chance to object and that such sub-processors are to be committed to all obligations set out within the data processing agreement between the controller and the processor; (e) appropriate technical and organisational measures need to be taken in order to assist the controller in responding to requests of data subjects exercising their rights; (f) the controller should be supported in complying with the obligations of notifying and communicating breaches, as well as the performance of Data Protection Impact Assessment; (g) all personal data needs to be deleted or returned after the provision of services has ended by choice of the controller, unless further storage is required by Union or Member State law; and (h) all information necessary to demonstrate compliance with the obligations of the Agreement needs to be made available to the controller, including a right for such to perform audits and inspections.

It should be noted that these are minimal requirements and that the parties are generally encouraged to include even more details governing their relationship and the processing activity, as well as the respective rights and responsibilities with regard to such.[323] Recital 81 also provides in that context, that while agreeing on specific stipulations by contract or legal act, account should be taken of the

---

[323] *EDPB*, Guidelines 07/2020, para 109; Rücker/Kugler, *Rücker*, B. Scope of application, para 169; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 64.

potential risks to the rights and freedoms of the data subjects which might result from such a processing activity and the specific tasks and responsibilities taken over by the processor in that regard. In this sense, the outsourcing of particularly high-risk processing activities concerning vulnerable data subjects, special categories of personal data, monitoring of public areas, or any other characteristics leading to the potential materialisation of serious ramifications will require a more detailed outline of certain aspects such as commitments of confidentiality, the authorisation of sub-processors, or technical and organisational measures.[324]

cc) Standard Contractual Clauses

Article 28(7) and (8) also allow the European Commission and the supervisory authorities of the Member States to issue standard contractual clauses regulating the above outlined stipulations between the parties. Such clauses have to be issued in accordance with the examination procedure of Article 93(2) and the consistency mechanism described in Article 63, respectively. The European Commission first published such a model contract on June 4, 2021.[325] The use of this pre-approved contract has the great advantage of legal certainty as well as easier implementation in comparison to individually negotiated contracts.[326] In order for the parties to rely on the legal certainty provided by this EU Act they are, however, not allowed to make any amendment to the clauses except for the selection of specific modules or options offered in the text, the completion of text

---

[324]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 81; *EDPB*, Guidelines 07/2020, para 110.

[325]Directorate-General for Justice and Consumers, *Standard contractual clauses for controllers and processors in the EU/EEA,* https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en (accessed: 20 October 2025).

[326]*New Standard Contractual Clauses - Questions and Answers Overview,* https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf, 5 (accessed: 20 Ocotober 2025).

where necessary and indicated accordingly, the filling out of the provided Annexes, and the addition of safeguards increasing the level of protection for the data.[327] A set of standard contractual clauses referred to as "DK SA Standard Contractual Clauses" was also proposed by the Danish Data Protection Agency and was published in January 2020[328] after taking into consideration the Opinion of the European Data Protection Board.[329] This was issued based on the initially submitted draft. While other DPAs also *often* provide for model contracts on their respective websites,[330] it should, however, be noted that such cannot considered "standard contractual clauses" as long as the consistency mechanism in accordance with Art. 63 is not being complied with and therefore will not have the same benefit of legal certainty.[331]

b) Direct Obligations

Additionally, to the extensive obligations which need to be included in the data processing contract in accordance with Art. 28(3), the GDPR also imposes a number of additional obligations directly onto the processor which were not present under the Data Protection Directive. Certain duties which result from Art. 28(3) such as obligations of confidentiality or assistance of the controller in ensuring compliance, have already been mentioned above. Others, however, are scattered throughout the entire Regulation.

---

[327]New Standard Contractual Clauses - Questions and Answers Overview, https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf, 6 (accessed: 20 Ocotober 2025); *EDPB*, Guidelines 07/2020, para 105.

[328]*EDPB*, DK SA Standard Contractual Clauses.

[329]*EDPB*, Opinion 14/2019.

[330]See for example: Bayerisches Landesamt für Datenschutzaufsicht, https://www.lda.bayern.de/media/muster_adv.pdf (accessed: 20 Ocotober 2025); Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/200429_AVV-Muster_DE.pdf (accessed: 20 Ocotober 2025).

[331]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 92; Paal/Pauly / *Martini*, Art. 28 DSGVO, para 73f; *Müthlein*, 2 RDV 2016, 74, 85.

aa) Record of Processing Activities

Article 30(2) provides that processors should maintain a record of processing activities, carried out on behalf of other controllers. While the extent of the information which needs to be documented therein is significantly limited in comparison to the ROPA required by controllers, it can still be characterised as quite considerable. Namely, such a record has to include: (a) the name and contact details of the processor and each controller on behalf of which they are acting; (b) the categories of processing activities performed for them; (c) where applicable, information on third country transfers and the suitable safeguards applied; and (d) general descriptions of the technical and organisational measures implemented in accordance with Art. 32(1).

bb) Technical and Organisational Measures

Article 32(1) creates an obligation for controllers and processors to implement technical and organisational measures for the purpose of ensuring the security of personal data. This level of security should be "appropriate" to the potential risks. When assessing the "appropriateness" of such measures the Article asserts that elements such as *"the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons"*, should be taken into account. The explicit inclusion of processors into the scope of this obligation was not previously part of the corresponding Art. 17 of the Data Protection Directive. It can, however, be argued that the obligation still existed indirectly, since Article 17(3) provided that the contract or legal act binding controller and processor should stipulate that the obligations for the assurance of appropriate technical and organisational measures should also be incumbent on the processor. The same rule has been included in Art. 28(3)(c) which also creates a need for the data processing agreement to include a requirement for processors to take all measures required pursuant to Article 32. Whereas at a first glance this may seem to make the direct inclusion of processors as duty holders under Art. 32(1) redundant in a sense, it serves a quite important purpose as it ensures that even where the contract fails to address these

issues or no contract is concluded whatsoever, the same legal obligations still applies, making the entity liable for any failings in that regard.[332]

cc) Breach Notification

In accordance with Art. 33(2), processors also have the obligation to notify the controller of a personal data breach after becoming aware of it, without undue delay. In that sense, the overall responsibility for handling and reporting the breach, where necessary, still lies on the side of the controller.[333] Notifications could, however, be made by a processor where the controller has authorised them accordingly as part of the data processing agreement.[334] It is, in any case, advisable to contractually designate the respective responsibilities of each party in the case of a security incident in advance, since the Regulation itself provides little details with regards to the actual content of the notification by the processor and their specific responsibilities in handling a breach.[335] Processors are, in principle, also not obliged to make any assessments regarding the likelihood or severity of any risks which might result for the affected data subjects prior to notifying the controller.[336] They are, however, expected to support the investigations of the incident as far as possible.[337]

dd) Designation of DPO

The instances in which the designation of a Data Protection Officer (DPO) by an entity becomes mandatory, as laid down in Article

---

[332]Schwartmann/Jaspers/Thüsing/Kugelmann / *Ritter,* 'Art. 32' DSGVO, para 20; Kühling/Buchner / *Hartung/Jandt*, Art. 32 DSGVO, para 4.

[333]*Art. 29 WP*, Guidelines on breach notification, 13; Kuner and others / *Burton*, Art. 33, 640, 647.

[334]*Art. 29 WP*, Guidelines on breach notification, 14; Gola/Heckmann / *Reif*, Art. 33 DSGVO, para 22.

[335]*Laue* / Spindler/Schuster, Art. 33 DS-GVO, para 22.

[336]Gola/Heckmann / *Reif*, Art. 33 DSGVO, para 22; *Laue* / Spindler/Schuster, Art. 33 DS-GVO, para 21; *Art. 29 WP*, Guidelines on breach notification, 13.

[337]Kuner and others / *Burton*, Art. 33, 640, 647; *Laue* / Spindler/Schuster, Art. 33 DS-GVO, para 22; *Art. 29 WP*, Guidelines on breach notification, 13.

37(1), apply as equally for processors as they do for controllers. This means that where a processor constitutes a public authority or body, except for courts acting in their judicial capacity where the core activities of such require regular and systematic monitoring of data subjects on a large scale or where they consist of processing on a large scale of special categories of data or personal data relating to criminal convictions, such an entity will also be required to appoint a DPO. This obligation exists independently from the duties allocated to the controller. It might, therefore, be possible for such a designation to be mandatory for one party but not the other.[338] A person selected for this function by the processor will also naturally bear the responsibility of overseeing any processing activities that are being performed within the entity in the function as controllers.[339]

Processors are also not only required to designate a DPO where the stipulations of Art. 37(1) are met but they also need to ensure that such a person is in a proper position to fulfil their duties as is laid out in Art. 38. In that sense, processors are also obliged to: make sure the DPO is properly and timely involved in all questions relating to the processing of protection of personal data (Art. 38(1)); support them in performing their task by providing the necessary access and resources (Art. 38(2)); guarantee that the DPO reports directly to the highest management level and is neither penalised nor receives any instructions with regard to the exercise of his or her tasks (Art. 38(3)); and eliminate any potential conflicts of interest which might result from those tasks (Art. 38(6)).

ee) Data Transfers to Third Countries

Article 44 of the GDPR provides that any transfer of personal data subject to the Regulation is only permitted where an adequate level of protection of natural persons can be provided. The obligation to assure such applies as equally to processors as it does to controllers since Art. 44 clearly states that any such transfer should only take

---

[338] *Art. 29 WP*, Guidelines on 'DPOs', 9; Kuner and others / *Burton*, Art. 37, 688, 693.

[339] *Art. 29 WP*, Guidelines on 'DPOs', 10.

place where *"the conditions laid down in this Chapter are complied with by the controller and processor*".

Similarly, as already outlined in the context of the direct obligation to provide for the existence of appropriate technical and organisational measures, the responsibility for securing any transfers of personal data to third countries or international organisations is already implied in Article 28 and that in multiple ways. First of all, Art. 28(2) introduces the requirement to obtain a prior written authorisation for the engagement of any type of sub-processors, which means that where such is located in a third country, the transfer would have to be authorised and thereby previously verified by the controller. Secondly, Art. 28(4) provides that where another processor is being engaged for certain processing activities, all the stipulations of Paragraph 3 need to be imposed on such an entity as well, especially with regards to the assurance of sufficient guarantees for the compliance with the regulation through implementing appropriate technical and organisational measures. In consequence, if the compliance of a sub-processor with the GDPR needs to be guaranteed, this would naturally also include the stipulations of Chapter V.

Finally, and most importantly, Art. 28(1)(a) directly refers to third country data transfers as it outlines that the documented instruction of the controller, in accordance to which the personal data is to be processed, also must include information on such, effectively prohibiting any transmissions from taking place without the direct authorisation of the controller. The only exemption applies where a requirement to a specific data transfer is directly enshrined in EU or Member State law. Here, the processor is, however, still generally obliged to inform the controller about this necessity in advance, unless the law in question specifically prohibits that. To what extent a processor, subject to such a direct legal obligation, would still be considered as such or rather take the position of a controller could, however, be debated as such an entity would consequently be granted their own legal basis for the processing of personal data (Art. 6(1)(c)). While this scenario is not to be equated to the change of roles referred to in Art. 28(10), since here an infringement of the Regulation would

need to materialise, the processor would effectively act outside the scope of the controller's instructions.[340]

Regardless, however, of the legal classification of such instances it can be concluded that Art. 28 does already essentially introduce an obligation for the processor to comply with Chapter V as a result of their dependency on the controller's instructions and authorisations. The direct applicability of the rules governing data transfers to third countries for processors enshrined in Art. 44 does, however, still serve an important purpose. First of all, similarly as with the case with Art. 32(1), it guarantees that where the controller fails to address these issues, either as part of the contract or their otherwise documented instructions, the obligation to assure appropriate safeguards for the rights and freedoms of the data subject still applies. Secondly, it supports the notion that processors, while in principle having to adhere to the controller's commands, should still analyse and consider the compliance of the processing activities outsourced to them within the scope of the Regulation. This is also supported by Art. 29(3) which states that processors have to inform the controller if they consider that the instructions they have received might infringe data protection law.

2. Consequences

Similarly, as has been previously outlined in the context of controllership, there are two basic types of consequences which might arise for entities as a result of incompliance with the requirements of the Regulation. These are namely measures imposed by the data protection authorities or direct liability for suffered damages towards individuals.

a) Powers of Data Protection Authorities

In principle, all the powers given to supervisory authorities by Article 58, enabling them to efficiently carry out their tasks outlined in Art. 57, can be utilised equally against processors, as well as

---

[340] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO, para 65.

controllers.[341] Such an applicability of these sanctions to processors is after all necessary for the assurance of the effective protection of the individual's rights and freedoms, since otherwise the DPAs would have no tools to correct, stop, punish, or otherwise intervene where processing of personal data is being conducted in a form not compatible with the requirements of the GDPR. In that sense, section A. VI. 2. a) Powers of the Data Protection Authorities can be largely referred to for details on the investigative powers, corrective powers, and authorisation and advisory powers which might be employed against processors.

The only differences occur where a power is specifically connected to an obligation only applicable to controllers. This is, for example, the case when it comes to the ordering of the communication of a personal data breach to the data subject under Art. 58(2)(e). Since this should exclusively be handled by the controller, supervisory authorities cannot demand processors to do so. Similarly, the option to advise in accordance with the prior consultation procedure referred to in Art. 36 also applies only to controllers (Art. 58(3)(a)), since processors are only required to assist them in conducting a Data Protection Impact Assessment but not perform such themselves (Art. 28(3)(f)).

b) Liability

Whereas the potential sanctions which may be issued by the supervisory authorities are, to a large extent, identical for controllers and processors there are, however, significant differences when it comes to the liability for damages suffered by individuals under Art. 82. As has already been evidenced above, the GDPR seriously widened the responsibilities of data processors in comparison to the previously applicable Data Protection Directive. Arguably the biggest change with regard to the legal position of such is, however, precisely the introduction of direct liability of the processor, as in accordance with Article 23 of the DPD, controllers were the only liable parties for

---

[341] *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 58 DSGVO, para 1.

damages resulting from an unlawful processing operation or any act incompatible with applicable data protection law.[342] The extent of the processors' liability, as well as their relationship with the controller in that regard, should therefore be discussed in this thesis.

aa) Eligibility and Damages

In accordance with Art. 82(1), the right to receive compensation for their suffered damages can be asserted by "any person". As has already been discussed above under Part 2 Chapter 3: A. VI. 2. b) aa) Eligibility, this right might only be limited to natural persons. The notion of restricting its applicability only to data subjects should, however, not be followed, since incorrect processing of personal data can also lead to significant losses for individuals, in particular when they are close to the data subject. Such a restriction could, therefore, potentially limit the effective protection of the rights and freedoms of individuals in a significant way.

Art. 82(1) also provides that claims for compensation can be made for both material as well as non-material damages. Whereas the assessment of material damages will typically be easier, immaterial damages are more likely to occur considering the rather intangible nature of the right to privacy and protection of one's personal data. Since at this stage there are no significant differences between claims made against controllers or processors, the above A. VI. 2. b) bb) Damages can be largely referred to for more details on the issues arising in the context of the determination and calculation of damages.

bb) Instances Giving Rise to a Claim

Article 82(2) introduces two instances under which processors can be held liable, namely when they have acted outside of or contrary to lawful instruction of the controller, or where they have failed to

---

[342] *Cordeiro*, 5 EDPL 2019, 492, 497; Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1165.

comply with obligations under the GDPR specifically directed towards them.

(1) Incompliance with Obligations

The obligations put on controllers by the General Data Protection Regulation (GDPR) have been outlined previously under Part 2 Chapter 3: A. VI. 1. Responsibilities. Most of these stem directly from Art. 28, which regulates the content of the contract with the controller (Art. 28(3)), as well as provides rules for the engagement of sub-processors (Art. 28(2) and (4)).[343] Another crucial responsibility introduced in Art. 28(3) is the duty of the processor to immediately inform the controller if they are of the opinion that one of the received instructions infringes on the GDPR or other data protection provisions. This assures that processors are not able to blindly act against applicable rules and regulations but, rather, they should to a certain extent be aware and critical of the orders given by their contractual counterpart.[344] The same rule was in fact already present in § 11(3)(2) of the old Federal German Data Protection Act (BDSG a.F.) and part of the commonly accepted practice in Germany that clearly unlawful instructions are not to be followed.[345] Where, however, the controller despite the voiced concerns still adheres to the instruction, the processor should be allowed to trust its legality unless the execution of such would lead to a clear and serious legal violation.[346]

Additionally, the GDPR also imposes a number of directly applicable obligations onto the processor such as: the maintenance of a record of processing activities (Art. 30(2)); the implementation of technical and organisational measures for the purpose of ensuring

---

[343]Ehmann/Selmayr / *Nemitz*, Art. 82, para 57; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 28; Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 6.

[344]Taeger/Gabel / *Moos/Schefzig*, Art. 82 DS-GVO, para 68; Gola/Heckmann / *Klug*, Art. 28 DSGVO, para 9.

[345]*Koós/Englisch*, 6 ZD 2014, 276, 281; *Müthlein*, 2 RDV 2016, 74, 76; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 79.

[346]Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 79; Taeger/Gabel / *Gabel/Lutz*, Art. 28 DS-GVO, para 60; Ehmann/Selmayr / *Bertermann*, Art. 28, para 33.

the security of personal data (Art. 32(1)); the notification of the controller of a personal data breach after becoming aware of it, without undue delay (Art. 33(2)); the designation of a Data Protection Officer, under certain circumstances (Art. 37(1)); and the assurance of appropriate safeguards in the case of third country transfers (Art. 44). Since Art. 58(2) also provides the supervisory authorities with the right to issue warnings, reprimands, and orders as well as impose specific limitations against controllers and processors, it can be assumed that the violation of such would also be considered as incompliant with the Regulation under Art. 82(2).[347] It is therefore evident that the instances, which might potentially give rise to a claim for compensation by an individual, are actually quite numerous and extensive.

(2) Act against Lawful Instructions

Processors will also be potentially liable for damages caused to a person where they have acted *"outside or contrary to lawful instructions of the controller"*. This instance, in a sense, logically follows the previous one. Since Art. 28(3)(a) clearly stipulates that the processors shall only process personal data based on documented instructions of the controller, any actions falling outside of such would constitute a lack of compliance with the Regulation. Where, on the other hand, the instructions are unlawful (as Art. 82(2) only included *"lawful instructions"* within its scope) the processor would either way, as outlined above, have to inform the controller of this in accordance with Art. 28(3). Where processors are unsure as to the legality of a certain duty imposed by their counterpart, they would, however, generally be advised to act in accordance with the orders of the controller in order to avoid liability, as refusing to act in accordance with instructions wrongly perceived as illegal could also lead to potential claims for compensation.[348] It should also be noted in that context that

---

[347]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 34.

[348]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 36; *Paal*, 1 MMR 2020, 14, 15.

where the actions of the processor go so far outside of the instructions of the controller that they must be regarded as a determination of the means and purposes of processing, the processor will in turn be regarded as a controller in accordance with Art. 28(10), thereby potentially making them liable to the same extent as the originally intended controller.[349]

cc) Causation

In the same vein, as is the case in the context of any claims for liability against controllers in addition to the materialisation of damages on the side of an individual and the existence of an instance giving to such claim, which in the case of processors lies either in the infringement of obligations specifically directed towards them or in performing actions outside or contrary to the instructions of the controller, the Regulation also requires the establishment of a causal link between the inquired damages and the identified acts of the processor, as Art. 82(2) clearly refers to damages "caused by" such processing.[350] For an overview of the legal issues surrounding the determination of the existences of such a link we can largely refer to the considerations presented previously in Part 2 Chapter 3: A. VI. 2. b) dd) Causation, as they are virtually identical to those identified in the context of the controller's liability.

dd) Burden of Proof

In the same vein, as is the case in the context of any claims for liability against controllers in addition to the materialisation of damages on the side of an individual and the existence of an instance giving to such claim, which in the case of processors lies either in the infringement of obligations specifically directed towards them or in performing actions outside or contrary to the instructions of the controller, the Regulation also requires the establishment of a causal link

---

[349]Gola/Heckmann / *Gola/Piltz*, Art. 82 DSGVO, para 6; Taeger/Gabel / *Moos/Schefzig*, Art. 82 DS-GVO, para 70.

[350]*Van Alsenoy*, 7 JIPITEC 2016, 271, 286; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 41; Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1175.

between the inquired damages and the identified acts of the processor, as Art. 82(2) clearly refers to damages "caused by" such processing.[351] For an overview of the legal issues surrounding the determination of the existences of such a link we can largely refer to the considerations presented previously in Part 2 Chapter 3: A. VI. 2. b) dd) Causation, as they are virtually identical to those identified in the context of the controller's liability.

ee) Joint and Several Liability

Article 82(4) of the GDPR provides that where multiple parties are involved in a processing activity and responsible for the identified damages, each such controller or processor should be liable for the entirety of the damages incurred by the person in question. Thereby the GDPR essentially establishes a regime of joint and several liability of controllers and processors, to the extent that they are responsible for the unlawful processing which has been the cause of the damages.[352] Allowing the injured party to claim the entirety of the damages from either of the counterparties involved serves the purpose of assuring full and effective compensation for that person, as has been specified in Art. 82(4). In that sense, the provision can be considered as resulting from the fundamental right to effective judicial protection enshrined in Art. 47 of the Charter, in conjunction with Art. 8 therein, which established the right to personal data protection.[353]

Some sources have also described this type of liability regime as "cumulative" based on the fact that while the controller still holds the central responsibility for any wrongdoings occurring during the processing of personal data, the data subject is additionally given the

---

[351] *Van Alsenoy*, 7 JIPITEC 2016, 271, 286; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 41; Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1175.

[352] Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1176; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204; *Paal*, 1 MMR 2020, 14, 18; *Kohn*, 11 ZD 2019, 498, 501; Ehmann/Selmayr / *Nemitz*, Art. 82, para 58; Rücker/Kugler, *Schumacher*, D. General conditions, para 831.

[353] Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1177.

possibility of suing the processor as well, where such responsibility for the damages lies at least partly on their side.[354] The individual is therefore essentially given the choice as to which party they would prefer to claim damages from or whether to bring charges against both.[355] This selection is, however, not without its practical consequences since Recital 146 provides that where the controller and the processor are joined to the same judicial proceedings, compensation may be appointed based on the respective responsibility of the parties for the established damages in accordance with the rules applicable in the law of the specific Member State. In effect, this means that where individuals decide to put forward a claim against multiple parties, their liability will be proportional rather than joint and several.[356] This, however, can only apply as long as the full and effective compensation of the injured party is still ensured, as outlined in Art. 82(4) and again pointed out in Recital 146. In that sense, proportional liability can be viewed as quite problematical and unlikely to be applied in practice,[357] unless the automatic reversal to joint and several liability, in the case of payment default by one of the parties, would be included in the judgement.[358]

ff) Compensation

Taking into consideration the above-mentioned legal issues affiliated with proportional liability, injured parties should in principle retain the right to be awarded full compensation from either of the responsible parties. Art. 82(5) of the GDPR does, however, provide an option for the respective party, who has reimbursed the data subject for the full amount of the damages, to claim compensation from the other entities involved in accordance with their level of responsibility

---

[354] *Van Alsenoy*, 7 JIPITEC 2016, 271, 285.

[355] *Wybitul/Leibold*, 4 ZD 2022, 207, 209; *Van Alsenoy*, 7 JIPITEC 2016, 271, 285; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 57.

[356] Ehmann/Selmayr / *Nemitz*, Art. 82, para 62; *Paal*, 1 MMR 2020, 14, 18.

[357] Ehmann/Selmayr / *Nemitz*, Art. 82, para 63; *Paal*, 1 MMR 2020, 14, 18f.

[358] Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 58; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 34.

with regards to the damaging event. From a logical perspective, the same should also apply where one party has paid an amount of damages higher than their actual degree of responsibility for causing such, otherwise the parties would in a sense be forced to pay the full amount independently of the reimbursements provided by others in order to be allowed indemnity.[359]

Art. 82(5) further provides that the respective level of responsibility for the damages should be determined in accordance with the conditions outlined in Paragraph 2. This means that controllers will be held accountable for any infringements of the Regulation, whereas processors will be only to the extent that an obligation of the GDPR was specifically directed at them or that they have acted outside of or contrary to the controller's lawful instructions.[360] It should, however, also be noted in that context that in accordance with Art. 28(4), processors are fully liable for the performance of their sub-processors. This means that should the conduct of such a sub-processor be the ultimate cause of the incurred damages and should such an entity be unable to award compensation for such, the controller would have a right to be reimbursed by the processor who engaged them.[361] Based on that, it could also be argued that the processors should be fully liable for the performance of their sub-processors vis-a-vis the data subject.[362] On the other hand, data subjects should not be precluded from pursuing claims directly against such sub-processors where this lies in the interest of their full and effective compensation.[363]

---

[359]*Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 36; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 60.

[360]*Paal*, 1 MMR 2020, 14, 18; *Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 36.

[361]*Boehm* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 82 DSGVO, para 36; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 39.

[362]*Van Alsenoy*, 7 JIPITEC 2016, 271, 286.

[363]*Van Alsenoy*, 7 JIPITEC 2016, 271, 286

gg) Exemption

Article 82(3) provides the option for controllers and processors to be exempted from liability where they are able to prove that they are not in any way responsible for the event giving rise to the damages. Since this exemption applies to both controllers and processors equally, the considerations on the issue outlined under Part 2 Chapter 3: A. VI. 2. b) ff) Exemption can largely be referred to and do not need to be repeated.

IV. Intermin Conclusions: Processor

Article 4 No. 8 of the GDPR defines processors as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*. A processor needs to be a separate legal entity from the controller and the controller has the requirement to assure that they can provide sufficient guarantees to ensure the protection of the data subject's personal data before engaging them. The fundamental component of the designation as a processor, however, lies in the factor that the *processing of personal data* is being performed *on behalf of* another legal entity. This means that all considerations with regards to the relationship between two parties should solely focus on the processing activity and not refer to elements outside of the scope of them, unless they are directly affected.

The element which most frequently leads to practical challenges in the context of differentiation in the different roles of entities involved in the processing of personal data, is the factor of doing so "on behalf of another party". In principle, therefore, the relationship between the controller and the processor has been constructed as one of subservience, in which one party should be acting in accordance with the other's demands and directions. This also leads to fact that the party providing the instructions is also largely responsible for assuring compliance with applicable data protection rules and having to guarantee due diligence in the selection of their vendor. On the other hand, the processor should not be acting outside or contrary to any directions given by the controller, which is why Art. 28(3) clearly

provides that they should only be operating *"on documented instructions from the controller"*.

While the adherence to the controller's instructions constitutes a central prerequisite for the characterisation as a data processor in the meaning of Art. 4 No. 8 GDPR, there is also a general consensus that it is still possible to leave them with a certain amount of discretion regarding the specific execution of the commissioned processing operations. While most sources conclude that the processor should not be making any decisions with regards to the purpose of the processing, a quite wide margin of discretion is often left when it comes to the means of such. Opinions on the specific degree often vary but many have by now accepted the division into "essential" and "non-essential" means, originally introduced by the WP 29. Both literature and Data Protection Authorities have also suggested the use of certain indicators for delimitation between the different roles of the parties such as, for example: who has the legal basis for processing, what types of data subjects are being targeted and what their relationship with the vendor is, how detailed the instructions given to the contractor are, to what extent the provision of the service is being supervised or monitored, or whether the service provider has particular expert knowledge in the field.

As has been the case with controllership, there are naturally a number of legal stipulations which result from being considered a processor in accordance with Art. 4 No. 8 GDPR. First of all, the relationship between the parties needs to be governed by contract or legal act which needs to be concluded in writing and has to contain a number of stipulations outlined very specifically and with great detail in Art. 28(3). Additionally, the GDPR imposes a number of direct obligations upon processors such as, for example, maintaining a record of processing activities, implementing technical and organisational measures for the purpose of ensuring the security of personal data. notifying the controller of a personal data breach after becoming aware of it without undue delay, designating a Data Protection Officer under certain circumstances, and assuring an adequate level of protection for the personal data in the case of third country transfers.

Where the processor might be incompliant with the obligations put forward in the GDPR, they may either be subject to measures imposed by the data protection authorities or direct liability for suffered damages towards individuals. In principle, all of the powers given to supervisory authorities by Article 58 can be utilised equally against processors as controllers, with the small exception of such relating to specific obligations of the latter. There are, however, significant differences when it comes to the liability for damages suffered by individuals under Art. 82. Whereas controllers can be held liable for any infringement of the Regulation, processors' claims can only be directed against processors where they have acted outside of or contrary to the lawful instruction of the controller or where they have failed to comply with obligations under the GDPR specifically directed towards them.

Where multiple parties are involved in the processing of personal data, Art. 82(4) establishes a regime of joint and several liability of such, as it provides that each should be liable for the entirety of the damages incurred by the person in question. While Recital 146 also theoretically allows for the distribution of proportional liability in instances where multiple parties are joined in the same judicial proceedings, the practical effect of this rule is likely to be limited due to the requirement of assuring full and effective compensation, introduced in Art. 82(4). Art. 82(5) of the GDPR does, however, provide an option for the respective party who has reimbursed the data subject for the full amount of the damages, to claim compensation from the other entities involved in accordance with their level of responsibility regarding the damaging event.

Whereas controllers are therefore to be considered the central figure when it comes both to decisions with regards to the processing of personal data, as well as the responsibilities resulting from this authority, processors rather take the role of a supporting character as any activities taken by them will be solely dependent on and on behalf of the controller. It should, however, be noted that the position of the processor has changed quite significantly in comparison to their legal status under the Data Protection Directive. Most importantly, they have been given a number of new obligations and

are also directly liable towards the data subject. While this is not necessarily an advantage for the processors themselves, who have been given both more duties and risks as a result, this change does significantly strengthen the position of the data subject. It can also in a sense be read as an acknowledgement of the importance of their role, which, due to the currently rising trends in outsourcing, has only grown over the years.

C. Joint Controllers

Another type of role which may be taken by a party involved in the processing of personal data is that of a joint controller. In contrast to the previously described positions this one, however, is not explicitly defined in Article 4 but rather can be derived from the definition of "controller" found in Art. 4 No. 7, the pluralistic element of which establishes that the determination of the purposes and means of the processing of personal data can be done alone or jointly with others, thereby allowing for the existence of multiple controllers for one processing operation.

I. History of the Term

The definition found in Article 4 No. 7 GDPR containing the pluralistic element which expressly allows for multiple entities to jointly hold the controllership for one processing activity, was directly lifted from Art. 2(d) of the Data Protection Directive (DPD). The responsibilities that come with that role, which have been laid down in Article 26 of the GDPR, however, are new which is why this legal figure has drastically gained in significance, as well as practical applicability, since 2018.[364]

The reason for introducing more specific requirements can most likely be found in the history of the provision as this concept, which was not defined but solely mentioned in Art. 2(d) of the DPD, was

---

[364] *Radtke*, Gemeinsame Verantwortlichkeit, 40.

rarely used in practice.[365] And while the Guidance on data controllers and data processors published by the Information Commissioner's Office in 2014 did make that distinction and provided some advice for companies on how those concepts should be used,[366] the same cannot be said about most other data protection authorities.

This is particularly interesting looking at the German history of data protection law, where the protection of personal data has not been overlooked or downplayed. The first Federal Data Protection Act was enacted in 1990 and came into force on June 1, 1991,[367] even prior to the existence of the Data Protection Directive. The Federal Commissioner for Data Protection and Freedom of Information was formed in 1987, with state authorities following shortly after. Likewise, the different roles with regards to the processing of personal data were well known and the differentiation between controllers and processors intensely debated by scholars, which is evidenced by the sheer amount of publications,[368] as well as court decisions,[369] dealing with this particular question. Yet the legal figure of joint controllership was virtually ignored not only in company practice but also by literature and data protection authorities.[370] The reason for this might be that the previous version of the Federal Data Protection Act did not mention it explicitly, whereas § 11 contained comprehensive rules for commissioned data processing.[371] This "obscurity" of joint controllership, however, will

---

[365] *Voigt/von dem Bussche*, GDPR, 18.

[366] *ICO*, Data controllers and data processors, para 15.

[367] Gesetzt zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (BGBl. 1990 I Nr. 73 S. 2954).

[368] *Engeler*, MMR 651, 653f; *Eckhardt*, 3 CCZ 2017, 111, 116f; *Weichert*, 4 VuR 2017, 138, 140f; *Lachenmann*, Datenübermittlung, 38-68, 89 -115; *Pauka/Kemper*, 2 NZBau 2017, 71, 74f; *Buchner/Schwichtenberg*, GuP 2016, 218, 223f.

[369] OVG Schleswig, ZD 2014, 643; LG Oldenburg, NJW-RR 2014, 1315; BGH, BeckRS 2012, 05302; LSG Niedersachsen-Bremen, BeckRS 2012, 67231; LSG Niedersachsen-Bremen, BeckRS 2011, 77754; OVG Schleswig, NordÖR 2011, 501; VG Gießen, NVwZ 2002, 1531; OLG München, BeckRS 1999, 11133.

[370] *Dovas*, 11 ZD 2016, 512, 514.

[371] *Dovas*, 11 ZD 2016, 512, 514.

definitely not continue. EU lawmakers have made a clear statement by including Article 26 in the Regulation, underlining the relevance of this concept. The Court of Justice of the European Union seems to be in complete agreement, reinforcing its practical applicability in recent judgements.[372] Therefore, it needs to be carefully considered when defining roles and responsibilities for processing personal data.

II. Definition

A definition of joint controllership can essentially be derived from two Articles found in the General Data Protection Regulation: Art. 4 No. 7 and Art. 26(1). Article 4 No. 7 provides the foundation by establishing the characteristics of a controller, whereas Art. 26(1) specifies under which circumstances such an entity would be considered as a joint controller. It is therefore important to note that, whereas the previously described processor constituted a party in its own right completely separate from the controller, a joint controller is, in a sense, a subtype of a controller. This means that as a first step, it would need to be confirmed that a party is in fact to be considered a controller under Art. 4 No. 7 and only then the possibility of joint controllership under Art. 26 should be considered.[373]

1. Controller

In accordance with Art. 4 No. 7, a controller is *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*. This definition and all of its elements have been analysed at great detail under Point I. Controller, and should

---

[372]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388; Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.

[373]*Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720; *EDPB*, Guidelines 07/2020, para 47; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 16; Ehmann/Selmayr / *Bertermann*, Art. 26, para 5.

therefore simply be referred to. This also means that the entity in question cannot be a processor, as defined previously under II. Processor, meaning that they should not be processing personal data on behalf of someone else.

While this seems obvious, the differentiation between the two can be quite difficult in practice, especially where the processor has been given a large margin of discretion.[374] After all, it has been determined that processors can, at times, be considered to have a tangible impact on the way personal data is processed, especially in instances where functions are outsourced based on the experience, skills, and knowledge of the processor as is often the case when it comes to the outsourcing of IT services.[375] In that sense, in many instances a particular processing activity might not be possible without the processor's involvement. One can argue that the controller may at any time choose a different processor for the processing activity in question; the same, however, can be said for joint controllers. Unless member states create legal provisions requiring certain processing activities to be performed by two specific actors, the parties are always free to choose with whom to collaborate.

In order to solve this conundrum, the EDPD points out that while processors participate in the processing, they do so only on the behalf of the controller and not for their own purposes.[376] The principal element of joint controllership seems to therefore lie in the intent of the parties. They need to have a personal interest in the execution of the processing activity other than providing a service to someone. This significance of the "why" of the processing is also mirrored in the position that only a controller can determine the purposes of the processing, whereas processors might have a varying degree of inference over the specific means.[377] The focus on

---

[374]See Part 2 Chapter 3: B. II. 2. b) Margin of Discretion.

[375]Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 28' DSGVO, para 37f; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 38.

[376]*EDPB*, Guidelines 07/2020, para 53 and 60.

[377]See Part 2 Chapter 3: B. II. 2. b) Margin of Discretion.

the parties' intentions or rather motivation for the conduct of a certain processing activity further encumbers a clear cut differentiation between the different roles, as the internal motivation can neither be proven nor objectively determined.

A helpful criterion, also in a sense relating to the question of the purpose of the processing, can be the determination of a legal basis for the processing activity. Whereas Art. 28 essentially creates a permission for controllers to transfer certain tasks and responsibilities onto third-party providers, without the need for them to have their own legal basis for the processing of personal data in accordance with Art. 6, the same does not apply for Art. 26.[378] As a result, an entity will always need to have their own legal basis for processing in order to be considered a controller in any form.[379] This will especially be the case where a certain undertaking is processing personal data based on a legal mandate.[380]

2. Two or More

Once it has been determined that two or more natural or legal persons should in fact be regarded as controllers, the applicability of Art. 26 can be considered. Article. 26(1) stipulates that two or more controllers should be regarded as joint controllers where they jointly determine the purposes and means of processing. In consequence, it will, naturally, not be sufficient to establish the existence of one controller with regards to a specific processing activity, but at least two entities fulfilling such a role.[381] These parties also need to be separate legal entities from each other, since authority over a processing activity exercised by multiple individuals or parts of an organisation would still be considered as the actions of one

---

[378]Ehmann/Selmayr / *Bertermann*, Art. 26, para 23; *Dovas*, 11 ZD 2016, 512, 515; *Monreal*, 12 ZD 2014, 611, 615.

[379]Ehmann/Selmayr / *Bertermann*, Art. 26, para 23.

[380]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 25.

[381]Taeger/Gabel / *Lang*, Art. 26 DS-GVO, para 24.

controller.[382] Exceptions could only apply where a certain function or division has such a high degree of independence, especially when it comes to decisions regarding the processing of personal data, that they need to be considered a separate controller.[383] This is, for example, at times argued for roles such as the workers' council, staff committees, or even data protection officers.[384] Also, where multiple entities are legally separate but part of a larger cooperation, this does not preclude them from being considered joint controllers since the GDPR does not recognize an intra-group privilege.[385]

3. Joint Determination of Means and Purposes

As mentioned before, Article. 26(1) stipulates that two or more controllers should be regarded as joint controllers where they jointly determine the purposes and means of processing. This means that the before mentioned authority over the processing of personal data must not only lie with two different entities at the same time but they also need to realise that power together. The different forms in which such a communal decision-making power can materialise and the criteria for its identification will be analysed below.

a) Joint Purpose

The purpose is typically referred to as the "why" of the processing of personal data.[386] The EDPB also mentions in this context the dictionary definition as *"an anticipated outcome that is intended or*

---

[382] *Radtke*, Gemeinsame Verantwortlichkeit, 99; *EDPB*, Guidelines 07/2020, para 75; *Jung/Hansch*, 4 ZD 2019, 143, 146-148; *Ambrock*, 10 ZD 2020, 492, 493f.

[383] *Radtke*, Gemeinsame Verantwortlichkeit, 99; Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 73-78.

[384] *Möhle*, Verantwortlichkeit des Betriebsrats, 30-39; *Radtke*, Gemeinsame Verantwortlichkeit, 99; Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 73-78; *Maschmann*, 18 NZA 2020, 1207, 1207ff; *Meinhold*, NZA 2019, 670, 670ff.

[385] *Voigt/von dem Bussche*, GDPR, 18.

[386] Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 150; Ustaran / *Macmillan,* Chapter 4, 89; *Voigt/von dem Bussche*, GDPR, 19; *EDPB*, Guidelines 07/2020, para 33.

that guides your planned actions".[387] A joint determination of purposes will therefore be presented in instances where both controllers are processing the data for the same reasons, meaning that they are trying to achieve compatible or common goals.[388] This raises a number of questions with regards to the degree of explicitness required for such purposes. First of all, since the definition is inherently broad it is not entirely clear how specific these goals would need to be phrased in order to be considered as converging.[389] Would it, for example, be sufficient if both parties aimed at realising a publication on a certain topic or would it also be necessary for them to have the same motives behind such publication? Also, in how abstract terms could those goals be phrased? Would something like "for profit" or "for the improvement of the system" suffice in order to be considered as the same goal?[390] The amount of sources and guidelines in this regard is, unfortunately, still quite limited.[391]

There also seems to be some uncertainty regarding the extent to which the purposes, for which the parties process the information in question, do in fact need to be identical.[392] The EDPB, after all, does seem to allow for some margin of differentiation, stating that the entities involved may also pursue purposes *"which are closely linked or complementary"*.[393] While it is further clarified that the pursuit of pure commercial benefit by two parties would not suffice for the

---

[387] *EDPB*, Guidelines 07/2020, para 31.

[388] *EDPB*, Guidelines 07/2020, para 57; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 718.

[389] *Golland*, 07 K&R 2018, 433, 436; *Rothkegel/Strassemeyer*, 20 CRi 2019, 161, para 31; *Radtke*, Gemeinsame Verantwortlichkeit, 124.

[390] *Golland*, 07 K&R 2018, 433, 436.

[391] *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 718.

[392] *Golland*, 07 K&R 2018, 433, 436; *Rothkegel/Strassemeyer*, 20 CRi 2019, 161, para 31.

[393] *EDPB*, Guidelines 07/2020, para 58.

consideration as a "common purpose",[394] current tendencies seem to be in support of a quite flexible approach in that regard.[395]

b) Joint Means

There also needs to be multiple entities involved in the determination of the means of the processing of personal data in order for joint controllership to apply. Whereas the purposes of the parties involved need to be, to some extent, compatible this is not exactly the case when it comes to the determination of means. Here it is generally established that each of the parties may be involved in different forms at different stages of the processing activity.[396] In that sense, the parties are free to divide between themselves the various parts of the processing operations, without having to involve their counterparts in the technicalities of such. This is, for example, common practice in research projects (which are one of the textbook examples of joint controllership), where the various institutions involved may take over different parts of the overall endeavour.[397] Party A might, for example, collect information about participants through a questionnaire whereas Party B may conduct a clinical examination of their health status; Party C could subsequently conduct an interview regarding their evaluation of the conducted tests and Party D may be tasked with analysing the data collected by the other entities. In this scenario, all of the parties are working towards a common goal but are able to make individual decisions with regards to their area of responsibility within the overall projects. It is, however, important to note in this context, the various steps

---

[394] *EDPB*, Guidelines 07/2020, para 60.

[395] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 12; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 46; *Golland*, 07 K&R 2018, 433, 436; *DSK*, Kurzpapier Nr. 16, 4. See also the analysis of the CJEU Judgement on Wirtschaftsakademie and Fashion ID below.

[396] *EDPB*, Guidelines 07/2020, para 61; *DSK*, Kurzpapier Nr. 16, 2f; *Kremer*, 35 CR 2019, 225, 228; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 19.

[397] *EDPB*, Guidelines 07/2020, para 66.

taken for the identified common purpose should complement each other in the sense that they should all be necessary for the achievement of the jointly defined goal.[398] This element of necessity has also been furthered by the CJEU in the case of *Fashion ID*; there the website operator was considered a joint controller based on the fact that without the inclusion of the plug-in, the transmission of data would not have been possible.[399] Interestingly, however, here the processing activity was split into various stages,[400] in a sense going against the idea of achieving an overall common goal. The details, consequences and potential problems with this judgement will, however, be discussed in detail under Part 1 Chapter 1: C. III. 3. Fashion ID in the following sections. What also needs to be kept in mind is the previously mentioned differentiation between essential and non-essential since influence or decision-making power over non-essential parts of the processing activity will, in principle, result in consideration as a processor, rather than (joint) controller.[401]

c) Joint Determination

Arguably, the most crucial element when it comes to the establishment of joint controllership is the question of joint determination. This component implies that there needs to be an element of communication between the parties, a moment in which decisions are being made by them together.[402] It will therefore not be sufficient for two entities to be processing personal data in order to achieve the same goal, if there is no understanding or communication between them in that context. If they were acting

---

[398]*Kremer*, 35 CR 2019, 225, 228.

[399]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 78.

[400]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

[401]*Kartheuser/Nabulsi*, 11 MMR 2018, 717, 718; Ehmann/Selmayr / *Bertermann*, Art. 26, para 6.

[402]Ehmann/Selmayr / *Bertermann*, Art. 26, para 23; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 12; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 718; *DSK*, Kurzpapier Nr. 16, 3; *Radtke*, Gemeinsame Verantwortlichkeit, 158; *Kremer*, 35 CR 2019, 225, 228; *Jung/Hansch*, 4 ZD 2019, 143, 144.

"next to each other" rather than jointly and where their cooperation in achieving a goal would be circumstantial, such a scenario would not result in a joint controller relationship.[403] Likewise, it is in principle not possible for a new entity to simply "join" an already established processing activity as a joint controller as this would amount to a new processing activity, the details of which need to be communicated to the data subject.[404]

aa) Joint Decisions

The EDPB lays down in their Guidelines that the element of participation regarding a particular processing activity, necessary for the qualification as a joint controllership, can materialise in the form of common or converging decisions.[405] Based on that distinction, joint participation will come in the form of common decisions, which provide the most basic form of understanding of the term "jointly", where the parties decide together on the relevant elements of the processing of personal data.[406] The idea of joint participation in the form of converging decisions is, on the other hand, slightly less intuitive and is largely based on ideas established in the case law of the CJEU, which will be analysed in details below. Here the EDPB explains that *"[d]ecisions can be considered as converging on purposes and means if they complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing"*.[407] The idea, therefore, seems to be that even where the parties are not explicitly making decisions with regards to each part of the processing together, they might still be "jointly" participating in the overall processing activity if the respective areas of responsibility are connected and impacting one another.

---

[403]Ehmann/Selmayr / *Bertermann*, Art. 26, para 23; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 12; *Kremer*, 35 CR 2019, 225, 228.

[404]*DSK*, Kurzpapier Nr. 16, 3.

[405]*EDPB*, Guidelines 07/2020, para 51.

[406]ibid para 52.

[407]ibid para 53.

The Board also further clarifies that when identifying a converging decision, it should be determined whether the overall processing activity would not be possible without the participation of all the involved parties, making them in effect inextricably linked.[408] A good example for such an instance might be the previously mentioned instance of a research project, where *often* different contributing entities will take over separate tasks lying within their respective areas of expertise.

bb) Distinction from Separate Controllership

The need for joint decision-making is crucial for the distinction of the different roles and responsibilities of the parties in the context of processing personal data. Whereas the element of determination constitutes the central factor for differentiating between controllers and processors,[409] the aspect of this determination taking place jointly is necessary for the distinction between joint and separate controllers, acting independently of each other.[410] This distinction is not only crucial but is also the cause of much confusion and is unfortunately often overlooked or even misunderstood by assuming that multiple actors involved in a processing activity need to either be in a controller-processor relationship or joint controllers.[411] This, however, could not be further from the truth, as it is more than common for multiple controllers to process the same personal data, use the same means of processing, or even pursue the same purposes without having any connection.[412] In that sense, where

---

[408]ibid para 53.

[409]See Part 2 Chapter 3: C. II. 1. Controller.

[410]Wybitul / *Tinnefeld/Hanßen*, Art. 26 DSGVO, para 8; *Radtke*, Gemeinsame Verantwortlichkeit, 157; *Colcelli*, 3 ECLIC 2019, 1030, 1036; *Kremer*, 35 CR 2019, 225, 228; *Jung/Hansch*, 4 ZD 2019, 143, 144.

[411]*Härting*, ITRB 2018, 167, 167f.

[412]For example, multiple entities might have access to the same database and even use it for the same general purpose, such as recruitment, but will do so completely independently of each other and solely for their own interests. Another example can be found in the everyday exchange of business contact details. While doing so both individuals acting on behalf of a company pursue the same goal: to

various entities are, for example, attempting to achieve the exact same purpose such as the development of a product or tool and personal data is being processed as part of that development process, they will naturally not be considered as joint controllers; in this case, each is simply working on their own project in their own interest, without any form of collaboration. Arguably, the same would also be true where different parties might be agreeing on the means of processing personal data and intentionally doing so together for completely different purposes.[413] Such a situation is, however, less straightforward and the actual roles of the parties will likely also be dependent on other factors.

d) Alternative or Cumulative Conjuction

The above-mentioned problem, in distinguishing between joint and separate controllers, also relates to another question, namely whether the joint determination of "purposes and means" constitutes an alternative or a cumulative conjunction and if, therefore, the parties need to agree on both in order to be classified as joint controllers, or if the common determination of one of the elements is sufficient.[414] The original Art. 29 Data Protection Working Party's Opinion 1/2010 on the concepts of "controller" and "processor" clearly stated that either purposes or means need to be shared by the parties.[415] The wording used in the Guidance of the European Data Protection Board, however, seems to support the idea that both components need to be present.[416] While the EDPB Guidance

---

stay in touch with the representative of the counterparty; however, each of them will do so separately on behalf of their company, in accordance with the rules and procedures applying there.

[413] *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 719; *Kremer*, 35 CR 2019, 225, 227.

[414] *Radtke*, Gemeinsame Verantwortlichkeit,130; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 718; Gola/Heckmann / *Piltz*, Art. 26 DSGVO, para 4.

[415] *Art. 29 WP*, Opinion 1/2010, 19.

[416] *EDPB*, Guidelines 07/2020, para 50: "*More specifically joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by*

officially replaced the Opinion of the WP29,[417] it does seem odd not to mention such a drastic change, or to not include more specific wording as to avoid any doubt on the reader's side. On the other hand, the assumption of an alternative conjunction would in turn lead to even more difficulties when trying to differentiate between joint and separate controllers. Most of the literature seems to, therefore, be in support of the fact that both parties need to agree on purposes and means cumulatively;[418] it should, however, be noted that there is also some support of a different view.[419]

Opting for the cumulative interpretation does not, however, mean that the parties need to agree on each and every detail of the processing. Quite the opposite is true, since it will very rarely be the case that both actors will be involved in the processing to the exact same extent. Entities might be responsible in different stages and divide the various tasks between each other, based on their expertise.[420] Typical examples can again often be found in the area of scientific research, where multiple institutions might work on one project but will fulfil completely different functions at different stages. An example of this is a clinic or laboratory collecting samples, where multiple institutions will subsequently analyse those in a pseudonymous form in order to draw conclusions for a paper which is to be published in the form of a collaboration. Here, while the processing activities performed by the individual actors are quite different, they are all working towards the same goal and will still need to agree on certain basic principles regarding the processing of personal data, such as the pseudonymization technique, the keyholder, the means used to transfer data, and the retention period.

---

all entities concerned, they should be considered as joint controllers of the processing at issue".

[417] *EDPB*, Guidelines 07/2020, para 4.

[418] Gola/Heckmann / *Piltz*, Art. 26 DSGVO, para 3; *Lee/Cross*, 9 MMR 2019, 559, 561; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720; *Radtke*, Gemeinsame Verantwortlichkeit, 132; Sydow/Marsch / *Ingold*, Art. 26, para 4.

[419] Rücker/Kugler, *Rücker*, B. Scope of application, para 145; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 18.

[420] *EDPB*, Guidelines 07/2020, para 55 and 61; *Bassini*, BLP 2019, 103, 120.

This decision-making process therefore renders the stakeholders as joint controllers.

e) Functional Concept

Since these are all functional concepts, they need to be interpreted according to the actual factual circumstances, leaving room for various arrangements between the parties. It would be possible for the research institutions from the previous example to simply determine all the necessary types of data they need collected and to then commission a laboratory to collect certain data points, which would be organised according to specific instructions and afterwards handed over to the research institutions. In that case, the laboratory would not be considered a joint controller but rather a processor, since they would not be pursuing any own interests regarding the processing, other than being paid for a certain service.[421] In another scenario, a clinic might collect data from individuals based on broad consent which is given for scientific purposes in general,[422] where data subjects agree that their information may be used or shared with different research facilities via a common platform. In this set-up, all of the actors will most likely be regarded as separate controllers even though they would be processing the exact same personal data and probably even for the same, or at least very similar, purposes. Since, however, none of these would be determined jointly, nor does any of the parties receive or give instructions to any other entity, they could neither be joint controllers nor processors.[423]

The above scenarios clearly illustrate how crucial it is to perform an in-depth analysis of the particular circumstances of each case and the actual influence each of the actors has on the processing activity.[424] It should also be noted that more often than not, defining

---

[421] *EDPB*, Guidelines 07/2020, para 60.
[422] *Hänold*, 1 ZD-Aktuell 2021, 05016; *Hänold*, 2 ZD-Aktuell 2020, 06954.
[423] *EDPB*, Guidelines 07/2020, para 68.
[424] *EDPB*, Guidelines 07/2020, para 12, 19, 20, 49, 67 and 80.

the specific role the parties take is more a matter of assessing the extent of their involvement on a scale, rather than being able to draw clean lines as cooperation and influence can take different forms.[425]This practice, however, unsurprisingly often leads to uncertainties and quite different views when it comes to the designation of legal status.[426] This controversy can also be seen in the decisions made by Data Protection Authorities, as well legal cases regarding these questions. The three most important and also most notorious court cases relating to this, shall be discussed in the following text.

III. Case Law of the Court of Justice of the Europea Union

As has already been mentioned, since the General Data Protection Regulation came into force, the legal figure of joint controllership has gained much prominence through the case law of the Court of Justice of the European Union. The three landmark cases of the last years which have not only received significant attention but are still being heavily debated are called *Wirtschaftsakademie Schleswig-Holstein*,[427] *Jehovan todistajat,*[428] and *Fashion ID*.[429] Since these were referred to the CJEU prior to the GDPR coming into force, the decisions were made based on the provisions of the Data Protection Directive. However as mentioned previously, the relevant definitions and general concepts regarding the division of responsibilities related to the processing of personal

---

[425] *Bassini*, BLP 2019, 103, 120.

[426]*Kartheuser/Nabulsi*, 11 MMR 2018, 717, 717; *Colcelli*, 3 ECLIC 2019, 1030, 1034; *Art. 29 WP*, Opinion 1/2010, 2; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 85.

[427]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388.

[428]Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551.

[429]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.

data have not changed, which means that these judgements are just as relevant to the current legal debate.[430]

1. Wirtschaftsakademie Schleswig-Holstein

On June 5, 2018, the Court of Justice of the European Union delivered its Judgement on a question which had arisen during the proceedings between the Independent Data Protection Centre for the State of Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; "the ULD") and the Wirtschaftsakademie Schleswig-Holstein GmbH (WAK). The question concerned the legality of the ULD's decision which had ordered the Wirtschaftsakademie to deactivate their Facebook fan pages, based on privacy concerns.[431]

a) Facts of the Case

The WAK is a private educational company, established in 1967, whose primary occupation concerns the offering of educational services.[432] As part of providing these services, the WAK had set up a fan page on Facebook.[433] The way this works is that both private and business users can register with Facebook and through their user accounts, create a page that promotes an underlying cause such as a particular service, business, or product. Creating such pages is extremely popular, especially among small and medium-sized enterprises, since it provides a relatively easy and free way to

---

[430]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, Opinion of AG Bobek, para 87; *EDPB*, Guidelines 07/2020, para 44; *Radtke*, Gemeinsame Verantwortlichkeit, 49; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 15; Wolff/Brink/v. Ungern-Sternberg / *Spoerr*, Art. 26 DSGVO, para 15; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 718; *Bassini*, BLP 2019, 103, 109, 120.

[431]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 2.

[432]More information available at: Wirtschaftsakademie Schleswig-Holstein, 'Lösungen für Unternehmen', https://www.wak-sh.de/unternehmen (accessed 23 October 2025).

[433]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 14.

reach a high number of users,[434] especially since fan pages can also be accessed by individuals who do not have a user account.[435] This means that such a page could be discovered over a search via a search-engine and subsequently accessed, without any barriers.[436] After accessing the page, Facebook will assign a unique user ID to the individual and information about that person will be collected via cookies and stored for a period of two years.[437] Administrators of fan pages can use a function called "Facebook Insights" which is free of charge and provides anonymous statistical data about the page's visitors.[438] This may include information about trends regarding age, sex, relationship status, occupation, lifestyle, and the interests of their audience,[439] thereby providing the means for more accurate and efficient targeting.[440] The conditions of use for this service are non-negotiable,[441] however, the administrator is able to define certain criteria for the creation of these statistics via filters made available by Facebook.[442] According to the order of reference, users were not provided with information concerning any of these processing activities.[443]

b) Course of the Proceedings

Based in the fact that fan page visitors were not informed regarding the cookie settings nor the further processing activities, on November 3, 2011 the ULD, which was the relevant supervisory authority in accordance with Article 28 of the Directive, issued its decision based on § 35(2) BDSG, ordering the WAK to deactivate its

---

[434] *Ahlden*, in: Social Branding, 43, 49.
[435] Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 41.
[436] *Radtke*, Gemeinsame Verantwortlichkeit, 50.
[437] Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 15.
[438] ibid para 15.
[439] ibid para 37.
[440] *Ahlden*, in: Social Branding, 43, 50.
[441] Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 15.
[442] ibid 36.
[443] ibid para 15.

Facebook fan page.[444] These proceedings were actually part of a larger campaign of the ULD, which had ordered multiple operators to cease their activity on the social-media portal.[445] The subsequent complaint issued by the WAK, which argued that it could not be made responsible for the processing of personal data conducted by Facebook, was denied as well.[446] The ULD held the position that setting up a fan page constituted an *"active and deliberate contribution"* to the processing of visitors' personal data, thereby making them liable as a service provider under § 3(3) No. 4 and § 12(1) TMG in conjunction with § 3(7) BDSG.[447] At the time, however, there was a significant backlash against this position from both the academic and political milieu which led to a deal being struck between the ULD and the parent company of the Wirtschaftsakademie, the Chamber of Commerce and Industry (Industrie und Handelskammer; "IHK"), which stipulated that the proceedings against the Wirtschaftsakademie were to be considered a "model process" for the question of social media fan pages and that until its finalisation, the Data Protection Authority would cease any other actions regarding this topic.[448]

After proceedings before the German Administrative Court (Verwaltungsgericht)[449] and Higher Administrative Court

---

[444]ibid para 16.

[445]*Weichert*, 42 DANA 2019, 4, 4.

[446]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 16f.

[447]ibid para 17.

[448]*Weichert*, 42 DANA 2019, 4, 4.

[449]The CJEU translates this as „responsible entity" (Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 19) which is correct in the literary sense, since „verantwortlich" means „responsible". A different translation is suggested here, since the term „responsible entity" was introduced specifically in order to include an equivalent to the term „controller" in German data protection law (previously it only had a "data storing entitiy" – "Daten speichernde Stelle") to ensure the correct implementation of the Data Protection Directive, as Germany had already been subject to a infringement proceedings (Gesetz zur Änderung des BDSG v. 18.05.2001, BGBl. I, 904); *Monreal*, 12 ZD 2014, 611, 614]. This translation is also consistent with the GDPR as the German translation of the term controller (Verantwortlicher) literally means "the responsible".

(Oberverwaltungsgericht),[450] the ULD finally appealed to the Federal Administrative Court (Bundesverwaltungsgericht) contending that their central argument, the fact that the operation of a fan page is to be considered a legally and technically homogenous process in which the operator and service provider depend on and complement each other, had not been acknowledged.[451] The Court basically supported the previous decisions, stating that the choice of a specific information and communications technology in itself could not amount to the role of a (joint) controller in the meaning of Article 2(d) of *Directive* 95/46/EC or § 3(7) BDSG (old).[452] It went on to explain that even when considering the possibility of pluralistic control, in which the joint participation of the parties may take different forms and does not need to be shared equally,[453] the ability to also determine the purposes and means of the processing still remains a formative and essential element of Article 2(d) of the Directive.[454]

While the court did not agree with the ULD's reasoning it did, however, recognise the need for a broad interpretation of the definition of a controller and/or controlling entity in the interest of effective protection of the data subjects' rights,[455] as well as the need for clarification as to the extent of responsibility of an entity in choosing the operator of its information.[456] It also raised some doubts regarding the ULD's exercise of powers, considering that Facebook Ireland was responsible for the collection and processing of personal

---

[450]OVG Schleswig, ZD 2014, 643, 643.

[451]Press Release: ULD, 'OVG-Urteil zu Facebook-Fanpages revisionsbedürftig', https://www.datenschutzzentrum.de/artikel/770-ULD-OVG-Urteil-zu-Facebook-Fanpages-revisionsbeduerftig.html (accessed: 23 October 2025). For more details refer to the original appeal: *Kauß*, Revisionsbegründung, https://www.datenschutzzentrum.de/uploads/facebook/Revisionsbegruendung-ULD-Gerichtsverfahren-facebook-Fanpages.pdf (accessed: 23 October 2025).

[452]BVerwG, ZD 2016, 393, para 27.

[453]As has been stated in: *Art. 29 WP*, Opinion 1/2010, 32f.

[454]BVerwG, ZD 2016, 393, para 27.

[455]ibid para 27.

[456]ibid para 31.

data,[457] and asked for clarification on the competence of supervisory authorities where a group company has subsidiaries in multiple European countries.[458] Last but not least, it established that there was uncertainty over the extent to which supervisory authorities are bound by decisions or appraisals of their counterparts located in other Member States.[459] Based on the identified issues, the Federal Administrative Court made the decision to stay proceedings and to refer six questions concerning the mentioned points to the European Court of Justice of the European Union (CJEU).[460]

c) Judgement

On June 5, 2018, the CJEU ruled on the submitted questions. Regarding those relating to the competence of supervisory authorities it established that (1) the supervisory authority of a Member State can exercise its powers over an entity, even if that entity is only responsible for marketing activities and an entity in another Member State is responsible for the collection and processing of personal data; and (2) that such a supervisory authority may exercise its powers of intervention independently from the supervisory authorities established in other Member States.[461] These two findings, however, while extremely important and relevant, shall not be further discussed here as they do not bear any relevance to the topic of this thesis.

What is, however, crucial for a full understanding of the term “joint controller” are the considerations and findings asserted by the Court in the context of the submitted Questions 1 and 2. Interestingly however, the referring court never asked whether or not the operator of a Facebook fan page was to be considered as a joint controller, since they appeared to be certain that this was not the case.[462] For

---

[457]ibid para 33.
[458]ibid para 40.
[459]ibid para 41.
[460]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 24.
[461]ibid para 75.
[462]BVerwG, ZD 2016, 393, para 27.

the Bundesverwaltungsgericht, the question revolved around alternative forms of liability for the selection of an operator of its information offering.[463] The CJEU began its considerations with a short reminder on the general purpose of the Data Protection Directive, which was the assurance of a high level of protection for the fundamental rights and freedoms of natural persons.[464] It went on to restate its previous findings, already established in the case of *Google Spain and Google*,[465] that the concept of controllership is to be interpreted broadly in order to assure *"effective and complete protection"* of the data subjects.[466] Furthermore, it underlined the fact that the definition of "controller", which included the element of "alone or jointly with others", clearly allows for the involvement of multiple actors taking part in the processing activity and therefore did not need to refer to a single entity.[467] The Court then went on to confirm the points which had not been subject to contention, namely that Facebook Inc. and Facebook Ireland were "controllers" for the processing activity in question, as they were the ones who primarily determined its means and purposes.[468]

After this introduction, the CJEU began its examination of the facts in order to determine whether and to what extent an administrator of a fan page actually contributed to the means and purposes of processing of personal data conducted by Facebook and whether this could potentially indicate that they would also be considered a controller under Art. 2(d) of Directive 95/46.[469] The Court contemplated that it would seem that a person, when creating a fan page on Facebook, concluded a type of contract with the social media provider and thereby agreed to the conditions of use for the

---

[463]ibid para 31.
[464]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 26.
[465]For details see above: A. I. 5. a) Google Spain.
[466]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 27f.
[467]ibid para 29.
[468]ibid para 30.
[469]ibid para 31.

webpage, including their privacy policies.[470] The processing activity, being the point of contention in the proceedings, is predominantly carried out by Facebook: It places cookies on the user's device, which store information on the browsers and in principle remain active for two years.[471] The data stored in the cookies is received, registered, and further processed by Facebook.[472] Their partners and even third parties may, however, make use of these cookies *"on the Facebook services to provide services [directly to that social network] and the businesses that advertise on Facebook"*.[473] The purpose of the processing activity mainly lies in enabling Facebook to improve its advertising system, as well as allow fan page administrators to receive anonymised user statistics so that they can manage their own promotional activities accordingly.[474]

With regards to the fan page administrator, the Court noted that simply using a social network did not necessarily merit the occurrence of joint controllership but that by creating a page, Facebook was essentially given the opportunity to place the cookies on the user's device, thereby enabling the collection of personal data.[475] It also established that the creation of such a fan page also required the definition of a number of parameters regarding target audience and the objectives of managing and promoting one's activities, which constituted a contribution to the overall processing of personal data by the administrator.[476] Furthermore, the administrator had the option to request demographic data concerning their target audience, including information regarding their age, sex, relationship status, occupation, and interests which essentially was equivalent to requesting the processing of this

---

[470]ibid para 32.
[471]ibid para 33.
[472]ibid para 33.
[473]ibid para 33.
[474]ibid para 34.
[475]ibid para 35.
[476]ibid para 36.

data.[477] While these statistics are provided in an anonymised form, the processing of such personal data is still necessary for their creation and the mere fact of not being able to access certain datasets does not preclude the possibility of being considered a controller.[478]

Based on these considerations, the Court of Justice of the European Union concluded that the administrator of a Facebook fan page does in fact take part in the determination of the means and purposes of processing by (1) defining the parameters for the fan page; and (2) having the objective of promoting its activities, thereby making them a controller in accordance with Art. 2(d) of the DPD, jointly responsible for the processing of personal data with Facebook Ireland.[479] The CJEU further underlined that although the type of social media provider was selected by the administrator for the purpose of benefiting from the associated service, it did not warrant an exemption from compliance with the obligations resulting from the applicable data protection law[480] and that the responsibility of the administrator was even greater in consideration of the fact that they might enable the collection of personal data for individuals without a Facebook account.[481] In that sense, the recognition of joint responsibility of both the Wirtschaftsakademie and Facebook for the processing operation in question was considered to be essential for the assurance of complete protection of the rights and freedoms of natural persons.[482] At the end of its analysis, the Court pointed out, however, that the parties were not to be considered as equally responsible for the processing in question, even though they were joint controllers.[483] On the contrary, the level of liability was to be

---

[477]ibid para 37.
[478]ibid para 38.
[479]ibid para 39.
[480]ibid para 40.
[481]ibid para 41.
[482]ibid para 42.
[483]ibid para 43.

assessed based on the factual circumstances of a case and the actual influence the parties have on the processing activity.[484]

d) Reception and Critique

The reception of this ruling can be described as mixed at best, with some acknowledging its purpose of assuring of a high standard of data protection[485] but many others taking significant issue with the findings of the Court.[486] It is, in fact, not hard to understand this stance since the CJEU's ruling seems to extensively broaden the term of what constitutes "joint controllers".[487] The reasoning that a fan page administrator will contribute to the processing by requesting the display of statistics and setting up parameters for their target audience in order to efficiently promote their services can easily be followed. It is also true that the WAK has its own purpose for the processing of personal data performed by Facebook, namely identifying trends within the target audience and therefore facilitating a more effective marketing strategy.[488] There are, on the other hand, a number of critical points which also need to be examined.

aa) Criticism

It is unclear where the Court sees the element of "joint" determination since as a matter of fact, there is no agreement or element of cooperation between the parties. It could be concluded that the court sees this element of joint determination in the implied contract which the parties enter into when an administrator opens such a fan page, since that administrator will thereby implicitly

---

[484]ibid para 43.

[485]*Berger/Eisendle*, 15 IJLT 2019, 20, 34; *Bassini*, BLP 2019, 103, 121; *Jung/Hansch*, 4 ZD 2019, 143, 144; *Weichert*, 42 DANA 2019, 4, 5.

[486]*Hacker*, 12 MMR 2018, 779, 779f; *Lee/Cross*, 9 MMR 2019, 559, 561; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 719f; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 94

[487]*Colcelli*, 3 ECLIC 2019, 1030, 1040; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 94; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 721.

[488]*Lee/Cross*, 9 MMR 2019, 559, 561.

subscribe to the terms and condition of the page.[489] This, however, would not be coherent since in the same paragraph, the court states that "it appears that" such a contract is being concluded and that this "is for national courts to ascertain",[490] thereby admitting that this is not a given. Based on that, the possible contract could not be the only element facilitating the element of cooperation between the parties. Also, even if the existence of such a contract was to be assumed, this would not in it of itself be sufficient for the determination of joint responsibility, as it has been established that these functional concepts are to be interpreted according to the actual circumstances at hand, meaning the actual relationship between the parties and not a (hypothetical) contract they entered into. Such a reading would also lead to the development of an excessive amount of constellations of joint controllership, thereby also making this legal figure completely derivative.

If, on the other hand, in accordance with the functional reading of the definition, we looked at the actual circumstances at hand there seems to be no real element of cooperation at all. The operator of the fan pages uses a Facebook service in accordance with pre-defined terms of use.[491] At no point is there any sort of agreement, negation, or discussion between the parties regarding the processing activity. Other than the establishment of certain limited parameters for the fan page and the request for statistics, the operator has virtually no control over the processing of personal data performed by Facebook and even the limited amount of control that is there exists only within the confines Facebook has set up and can at any point change.[492] This is also the conclusion that the German Courts drew previously and why they denied the existence of controllership

---

[489]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 32.

[490]ibid para 32.

[491]See also regarding the problem of a lack of influence of the subordinate party: *Hacker*, 12 MMR 2018, 779, 780.

[492]*Hacker*, 12 MMR 2018, 779, 780.

on the side of WAK.[493] Also questionable in this case is the presence of a joint purpose.[494] While the fan page operators are generally interested in evaluating the statistics in order to optimise their service offerings for the identified audience, the focus of Facebook lies on the provision of personalised ads of third parties to its users.[495]

As, however, the Federal Administrative Court had noted, the lack of controllership assumed by the previous courts would have in turn lead to a lack of protection of the rights and freedoms of the data subjects.[496] This also seems to have been the fear of the CJEU, which clearly stressed the need for *"effective and complete protection of the persons concerned"*[497] and later explained that the recognition of joint responsibility for fan page operators would help ensure a *"more complete protection"* of their rights.[498] It would therefore be reasonable to assume that this broadening, which is somewhat inconsistent with the letter of the law as well as the Art. 29 Working Party's Guidance, came as a result of the need to ensure a high level of data protection within the EU by closing the presumably identified legal gap.

bb) Suggested Solution

Interpreting the law in accordance with the purpose of the provision in order to ensure its effectiveness, the so called *"effet utile"*, is considered a traditional way of interpretation and frequently used by the CJEU.[499] It should, however, be questioned whether such an evasion of the letter of the law was in fact necessary.

---

[493]VG Schleswig, ZD 2014, 51, 51; OVG Schleswig, ZD 2014, 643, 644; BVerwG, ZD 2016, 393, para 27.

[494]*Kartheuser/Nabulsi*, 11 MMR 2018, 717, 719f.

[495]*Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720.

[496]BVerwG, ZD 2016, 393, para 33.

[497]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 28.

[498]ibid para 42.

[499]*Bergmann*, 'Effet utile' in HdLexEU; *Potacs,* 44 EuR 2001, 465, 465; *Sadl*, 8 EJLS 2015, 18, 22; *Fennelly*, 20 Fordham Int'l L.J. 1996, 656, 674.

As has been correctly established by the CJEU, the administrator of a FB fan page has a personal interest in running the page, namely promoting their product and optimising their marketing. They also have influence over the means of processing by setting certain parameters and as the German Federal Administrative Court pointed out in its first questions when it asked about the extent of the responsibility of an entity in choosing the operation for its information offering, a choice regarding the selection of an information service provider.[500] This element of determination, which realises itself in the choice of Facebook as the platform for promotion, was virtually ignored by the CJEU. However, this should be considered a significant component of the overall circumstances. It is here that we can see the real influence of the WAK over the processing activity; they are free to use other means of promotion and marketing but specifically decided to use a Facebook fan page for their purposes. While the Federal Administrative Court correctly identified the extent of the influence excreted by the WAK, they incorrectly assumed that there were not to be considered an entity controlling the processing within the meaning of Art. 2(d) of the Directive.[501]

As has been established under Part 2 Chapter 3: A. II. 3. Processing earlier in this thesis, the term “processing” may refer to both a singular operation or to a set of operations, which means that it can either entail one activity or a number of steps which are connected. While it is common practice for controllers to “bundle” a number of individual processing elements such as the collection of a dataset, its organisation, use, storage, access and deletion once the pursued purpose has been achieved into one overall processing activity for reasons of practicality, this is not a must. The condensation of multiple steps or repetitive actions into a singular activity is logical from the perspective of a specific entity, especially when creating a record of processing activities and since, thus far, there has been no guidance outlining any limitations in these regards, it can be assumed that the structuring of these activities is

---

[500]Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 24.
[501]ibid para 24.

left largely to the discretion of the controller, as long as all of the elements required in Article 30(1) can be depicted accurately and transparently (see Part 2 Chapter 3: A. II. 3. b) Processing Activity). This limitation in defining the term means that an extension, to the point by which processing operations performed for different purposes, based on a different legal basis and subject to different technical and organisational measures, are somehow consolidated into processing activity, should therefore not be possible.

When defining the processing of personal data being performed under the control as well as responsibility of the Wirtschaftsakademie, it should thereby be concluded that the relevant processing activity, which requires consideration in this context, is the administration of a fan page via the social network provider Facebook. In that sense, any content posted on such a page would be subject to the GDPR (or then the Data Protection Directive). Equally, any parameters set up by the fan page operator would fall under their responsibility, as would any requested statistics, regardless in which form they were being provided. The means and purposes of the processing of personal data for these elements were being determined by the WAK; they had an interest in promoting their activities and they decided on the use of a certain provider to do so.[502] If the use of a certain platforms is not possible in a GDPR compliant manner based, for example, on lacking technical and organisational measures to ensure a level of security appropriate to the risk (Art. 32) or insufficient guarantees for the level of protection of natural persons (Art. 44), a controller would simply not be allowed to use such means of processing and could be held liable for the selection they have made.

The artificial creation of a joint controllership, which would require a common determination of means and purposes between the parties at hand, is simply not necessary to assume responsibility on the side of the fan page operator, since there are sufficient grounds for the assumption of separate controllership.[503] The two processing

---

[502] *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720.
[503] *Lee/Cross*, 9 MMR 2019, 559, 562.

activities of the WAK and Facebook can be considered as completely separate processes, without allowing entities which select a certain social media platform or any other service provider for that matter, to circumvent data protection laws. Especially the duty to provide the data subject with the necessary information and the requirements for valid consent would be exactly the same, meaning that the assumption of joint controllership essentially does not even further the principle of transparency in any significant way.[504] The same would also apply for all of the other data subject's rights.[505] Also, while the assumption of separate controllership does limit the liability of the WAK to the processing of personal data under its control, it does not preclude the Data Protection Authorities nor the data subjects from pursuing claims directly against the platform. In that sense, it simply seems unnecessary to broaden the scope of joint controllership in such a significant and arguably erroneous manner in order to achieve the effective enforcement of data protection law.[506]

2. Jehovan Todistajat

The second landmark ruling of the Court of Justice of the European Union regarding the respective roles and responsibilities taken by different actors involved in the processing of personal data and in particular the legal figure of joint controllership, was issued only a month after the court's preliminary judgement on the case of the Wirtschaftsakademie on July 10, 2018.[507]

a) Facts of the Case

The case was concerned with the door-to-door preaching activities of the Jehovah's Witness community.[508] The members of

---

[504]ibid,
[505]ibid.
[506]ibid.
[507]Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551.
[508]ibid para 15.

that group would typically take notes during the course of such which contained information about the individuals they were visiting, including details such as names, addresses, religious beliefs, and family circumstances.[509] These notes were taken so that they could serve as a memory aid, as well as a conversation starter for the community members upon their subsequent visits.[510] The collection of such data was neither communicated towards the data subjects, nor was their consent obtained at any given point.[511]According to statements provided by the Jehovah's Witnesses, community members are not required to collect any data during their preaching activities.[512] The community also does not receive any information with regards to the content of the notes, which are of a rather informal nature.[513]

A certain impact of the community on the preaching activities of its members has, however, been established. First of all, the community provides its members with guidelines on how these notes should be taken, which appear in at least one of their magazines dedicated to the subject of preaching in general.[514] Secondly, the community and its congregation are responsible for the organisation and coordination of the preaching activities of their members as they provide a map of areas allocated between the respective individuals who engage in preaching.[515] Additionally, a record is kept about the preachers, containing information regarding the amount of publications distributed by them.[516] Furthermore, the community maintains a so called "refusal register", which constitutes a list of individuals who have explicitly requested not to be visited any more.[517] This list is utilised by members of the community in the

---

[509]ibid para 15.
[510]ibid para 15.
[511]ibid para 15.
[512]ibid para 17.
[513]ibid para 17.
[514]ibid para 17.
[515]ibid para 16.
[516]ibid para 16.
[517]ibid para 16.

context of their door-to-door preaching activities in order to avoid further approaching people who do not wish to be contacted. In the past, the Jehovah's Witness community has also distributed standardised forms among their members to be used for the collection of relevant data for this list.[518] Based on recommendations from the Data Protection Supervisor, the community has, however, ceased making these available.[519]

b) Course of the Proceedings

The proceedings in this case started in September 2013, when the Finnish Data Protection Board adopted a decision which prohibited the Jehovah's Witness community from continuing the collection or other forms of processing of personal data conducted by their members as part of their door-to-door preaching activities as long as the legal requirements under Finnish data protection law (Law No 523/1999) were not met.[520] The issued ban was based on the assumption that the actions taken by the community, as well as its members, constituted processing of personal data in the meaning of the applicable law and that both parties were to be considered as controllers in the context of such.[521]

This decision was challenged by the Jehovah's Witness community, who brought an action against it before the Administrative Court in Helsinki (Helsingin hallinto-oikeus).[522] The court annulled the decision, coming to the conclusion that the described activities did not constitute unlawful processing of personal data under Finnish data protection law and that the community was not to be considered a data controller in that context.[523] This judgement was subsequently challenged by the Data

---

[518]ibid para 16.
[519]ibid para 16.
[520]ibid para 11.
[521]ibid para 12.
[522]ibid para 13.
[523]ibid para 12.

Protection Supervisor before the Supreme Administrative Court (Korkein hallinto-oikeus).[524]

The Supreme Administrative Court based its considerations on multiple issues which were highlighted as requiring clarification. First of all, while the Court did support the notion that the actions taken by the community and their members constituted processing of personal data within the meaning of Article 3 of Directive 95/46, it also posed the question whether these were covered by the exception of Art. 3(2), which excluded processing performed in the course of a purely personal or household activity, from the scope of the Directive.[525] Secondly, it was uncertain whether these activities would fall under the scope of Art. 3(1) in conjunction with Art. 2(c) since based on these, the Directive would only apply to the non-automated processing of personal data where the information contained therein formed part of a filing system.[526] Finally, the question was raised whether the influence of the Jehovah's Witness community on the preaching activities of their members sufficed to consider them a data controller under Art. 2 (d).[527] Based on these doubts, the Supreme Administrative Court decided to stay the proceedings and referred four questions regarding the contemplated points to the Court of Justice of the European Union.[528]

c) Judgement

In its ruling, the CJEU concluded that processing of personal data carried out by the members of a religious community in connection with door-to-door preaching does not fall under either of the exemptions of Art. 3(2), as they are neither activities of state authorities nor carried out in the context of the private or family life of individual, as it is directed outwards from the private setting of the

---

[524]ibid para 14.
[525]ibid para 19.
[526]ibid para 20.
[527]ibid para 21-23.
[528]ibid para 24.

members.[529] While the applicability of the right to freedom of conscience and religion was considered and supported, the CJEU established that this does not automatically preclude such activities from falling under data protection law.[530] As for the interpretation of the term "filing system", the Court concluded that the information collected as part of the preaching activities fell under that definition regardless of the criteria used to structure them as the retrieval of the data, either for a subsequent visit or on order to avoid such where this has been demanded by the data subject, is part of the purpose of collecting it in the first place.[531]

Both of the matters analysed in Questions 1 and 2 are of great importance in the context of data protection law as a whole. For the purpose of this thesis, most attention should, however, be directed to Questions 3 and 4 which were submitted by the Finnish Supreme Administrative Court and ask whether or not the Jehovah's Witness community and its members are to be considered as joint controllers, in the meaning of Art. 2(d) of the Directive. In its analysis, the Court began by reiterating its crucial conclusion from its former judgement in the case of the *Wirtschaftsakademie*, stating that effective and complete protection of data subjects should be assured through the application of a broad definition of the concept of controller.[532] It also underlined again that joint responsibility should not be mistaken as implying equal responsibility and that the involved parties may bear responsibility for different stages of the processing, to different degrees.[533] This also meant that it was not necessary for each actor to have access to the relevant data in order to be considered a controller.[534]

With regards to the case at hand, the CJEU pointed out that while the individual members of the community freely determined which

---

[529]ibid para 39, 42, 44, 50 and 51.
[530]ibid para 46-49.
[531]ibid para 60 and 62.
[532]ibid para 66.
[533]ibid para 66.
[534]ibid para 69.

information to gather in the context of their preaching activities and how to utilise it in the future, the overall purpose of the entire process seemed to lie in supporting the objectives of the Jehovah's Witness community as a whole.[535] The community also acknowledged that and supported this goal by organising and coordinating the preaching activities of its members, through means such as the allocation of areas.[536] Based on that, the Court came to the conclusion that the door-to-door preaching was therefore encouraged by the community.[537] In light of these considerations, the CJEU determined that while the final decisions would need to be made by the referring court, in consideration of the overall circumstances, *"it appears that the Jehovah's Witnesses Community, by organising, coordinating and encouraging the preaching activities of its members intended to spread its faith, participates, jointly with its members who engage in preaching, in determining the purposes and means of processing of personal data of the persons contacted."*[538]

d) Review

In contrast to the prior ruling in the case of the *Wirtschaftsakademie*, the CJEU's decision on *Jehovan todistajat* has been generally accepted without any significant criticism, at least with regard to the main determinations on the definition of filling system and joint controllership.[539] This may be due to the fact that the Court did not come to any essentially new conclusions but rather reiterated their previous stance on the manner in which these terms

---

[535]ibid para 70-71.

[536]ibid para 71.

[537]ibid para 72.

[538]ibid para 73.

[539]Subject to debate however is the issue of governing religious communities through common data protection law, without considering their specific freedoms under international and Member State law. See for example: https://verfassungsblog.de/die-zeugen-jehovas-und-das-datenschutzrecht/ (accessed: 09 March 2026); *Hoeren*, 10 ZD 2018, 469, 472f.

are to be interpreted. Additionally, the facts at hand seemed significantly less contentious than before. After all, here the Jehovah's Witness community had a far clearer and easily established impact on the actual processing of personal data. There was also little dispute as to the fact that both the members and the overall community were following the same objective, thereby having a common purpose. This was far more questionable in the relationship between the WAK and Facebook.

What is, however, unfortunate in this context is the fact that no real consideration was given to the role of the members themselves. Since none of the referred questions concerned them, the Court simply concluded that since *"only the responsibility of that community is challenged, the responsibility of the members who engage in preaching does not appear to be called into question"*. More insight into the readings of that relationship and how it should be treated or formalised would in fact have been particularly relevant, especially in light of the new requirements introduced by the GDPR. While the Directive did not provide for any specific stipulations with regards to the legal figure of joint controllership, this has changed substantially under the GDPR, mainly through the introduction of Art. 26 and Art. 82(4) and (5). The specific consequences of joint controllership will be presented in detail below under Part 2 Chapter 3: C. IV. Effect. In short, however, the parties need to enter into a contract, outlining their respective responsibilities for compliance with the data protection obligations and will be held jointly and severally liable for any damages caused by their wrongdoing in that regard. In consequence, these obligations would therefore also need to apply to the Jehovah's Witness community and its members, forcing them to enter into a contract outlining their respective responsibilities under the GDPR.

This would also mean that individual members could potentially be held liable for the entirety of any damages caused by the community's misconduct. Such an outcome seems quite problematic, especially considering the potential dependency of the individuals on their religious community, as well as the trust that is typically put into them. The presence of this vulnerability has in fact

been indirectly recognised by the community itself. The Advocate General noted in his Opinion that they denied their role as a controller of the data collected and *"expressed some irritation at the statement that its members act on its instructions and not in response to divine command"*.[540] This belief in a "divine command" shows that there is a significant hindrance for individuals to actually assert any sort of control over the actions of their community, as there is likely to be in an inherent belief in the competence of their officials. The situation can, in a sense, be compared to the relationship between an employee and their employer. As outlined above, only "rogue employees" will be considered as data controllers in their own right (see Part 1 Chapter 1: A. I. 2. Natural Person). Typically, however, they will simply be regarded as acting "on behalf of" their organisation. Similarly, members of any religious community will act on behalf of their faith. There is, in most instances, a stronger internal motivator to do so when it comes to one's beliefs, whereas actions for an employer will often be motivated by more mundane reasons such as wanting to perform well in order to keep a position or even be promoted. In this case, the individual's actions in a moral imperative, in a sense, create an even higher level of dependency. Employees will typically be dependent financially on the organisation they work for and therefore feel required to act in accordance with the provided instructions, whereas members of a religious community or other form of organisation following moral guidelines or goals will feel an ethical obligation to act accordingly. In that sense, it should be questioned whether or not an autonomous element of "determination" can be present for such members or whether they would ultimately always be acting on behalf of and in accordance with the guidance (whether direct or indirect) of their respective community.

---

[540]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, Opinion of AG Mengozzi, para 61.

3. Fashion ID

The third crucial judgement of the Court of Justice of the European Union concerning the determination of joint controllership, as well as the central practical issue of differentiating such from separate controllers, was issued on July 29, 2019 and until this point, arguably constitutes the most pivotal ruling in the context of determining the respective rights and responsibilities of the parties involved in the processing of personal data.[541]

a) Facts of the Case

The German online clothing retailer Fashion ID had embedded a social "Like" plug-in from Facebook on their website, commonly referred to as a "Like button".[542] These types of plug-ins function in a way in that they constitute a direct link to the website where the original "Like button" is present, in this case Facebook.[543] This feature, allowing the browser to display content from different sources, is commonly used on the internet, for example, for the display of pictures, videos, news etc.[544] Such third-party content can be embedded by website operators onto their website by placing a link to the external source.[545] When an individual visits the operator's website, their browser identifies the link and automatically adds the content from the third-party provider to the appearance of the page.[546] In order for this functionality to work properly, the browser of the website visitor needs to transmit their IP address and the browser's technical data to the server of the third-party provider.[547] This is necessary for the server to establish in which format the

---

[541]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.
[542]ibid para 25.
[543]ibid para 26.
[544]ibid para 26.
[545]ibid para 26.
[546]ibid para 26.
[547]ibid para 26.

required content should be delivered to the address.[548] Furthermore, the browser has to transmit information regarding the content which is being requested.[549] It is impossible for the operator of a website, deciding to include such third-party content onto their offering, to control what kind of information is being transmitted by the browser or to what extent or how this data is being further processed by the third-party.[550] The Facebook "Like" button embedded in the website of Fashion ID functioned in such a way that each time an individual visited the Fashion ID website, their personal data was automatically transmitted to Facebook Ireland, regardless of whether or not such individual clicked the button and without their awareness.[551]

b) Course of the Proceedings

The described practice came to the attention of Verbraucherzentrale NRW, a public-service association responsible for the assurance of consumers' rights and interests.[552] They directed criticism towards Fashion ID for the transmission of personal data to a third party without obtaining the data subjects' respective consent as well as failing them in accordance with the requirements set out by data protection law.[553] In order to assure that Fashion ID ceased the data transfers which the Verbraucherzentrale considered to be illegal, they brought legal proceedings for an injunction before the Regional Court in Düsseldorf (Landgericht Düsseldorf).[554] The court in essence upheld this request, deciding that the Verbraucherzentrale had standing to bring proceedings under Paragraph 8(3)(3) of the UWG.[555]

---

[548]ibid para 26.
[549]ibid para 26.
[550]ibid para 26.
[551]ibid para 27.
[552]ibid para 28.
[553]ibid para 28.
[554]ibid para 29.
[555]ibid para 30.

In consequence, Fashion ID decided to appeal against that decision before the Higher Regional Court in Düsseldorf (Oberlandesgericht Düsseldorf), with Facebook Ireland intervening in the appeal in their support.[556] Fearing the continuation of the data transfer, the Verbraucherzentrale NRW subsequently bought a cross-appeal, aiming at the extension of the ruling made in the first instance.[557] In their appeal, Fashion ID argued that the decision of the Regional Court was incompatible with the Data Protection Directive based on two grounds.[558] Firstly, they brought forward that legal remedies were only granted to data subjects and supervisory authorities under Articles 22 and 24 of Directive 95/46, thereby making the action of Verbraucherzentrale NRW inadmissible.[559] Secondly, they argued that contrary to the assertion made by the Regional Court in Düsseldorf, they could not be considered as a data controller in the meaning of Art. 2(d) as they did not exert any influence over the transmission of personal data, the subject of the proceedings, nor over the way in which such data might subsequently be used by Facebook Ireland.[560]

The Higher Regional Court voiced some doubts with regards to the assertions made by Fashion ID.[561] Concerning the assertion of inadmissibility of the action of the Verbraucherzentrale NRW, the court took the view that Art. 24 did not give any reason to exclude such associations from bringing legal proceedings, as it expressly asked Member States to *"adopt suitable measures to ensure the full implementation of the provisions of this Directive"*, thereby allowing for the introduction of national legislation permitting such.[562] The court also pointed out that Art. 80(2) of the GDPR did in fact also provide not-for-profit bodies, organisations, or associations with the

---

[556]ibid para 31.
[557]ibid para 31.
[558]ibid para 32.
[559]ibid para 33.
[560]ibid para 34.
[561]ibid para 35.
[562]ibid para 35.

right to lodge a complaint and to an effective judicial remedy under Articles 77, 78 and 79 as well, suggesting a general tendency to support these types of actions by the lawmakers.[563]

Uncertainty was, however, voiced with regards to the question of whether or not a website operator such as Fashion ID could in fact be considered a controller under Art. 2(d), taking into account their lack of influence over the processing of personal data conducted by the third party provider.[564] The court also considered that if it was concluded that Fashion ID was in fact not a controller, whether an alternative form of liability under national legislation for the infringement of data protection rights, for example in the form of the German "Störerhaftung" (liability for disruption), was permissible.[565]

Finally, regardless of their role as controller or disruptor, a substantial amount of uncertainty was voiced with regards to the extent of the responsibilities on the side of Fashion ID.[566] This included the question of whether or not they did in fact have a duty to inform the data subject,[567] the legitimate interests of which parties had to be taken into account,[568] and who was required to obtain the necessary consent form the website users.[569] In consideration of all of these doubts with regard to the correct interpretation of the Directive, the court decided to refer six questions to the CJEU, concerning the described matters.[570]

c) Judgement

The Court delivered its Judgement on July 29, 2019.[571] As outlined before, six questions had been referred to the CJEU for

---

[563]ibid para 36.
[564]ibid para 37.
[565]ibid para 38.
[566]ibid para 39-41.
[567]ibid para 39.
[568]ibid para 40.
[569]ibid para 41.
[570]ibid para 42.
[571]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.

preliminary judgement, which concerned the lawfulness of actions taken by public-service associations against infringements of data protection law (Question 1); the legal designation of the website operator as a controller, with regards to the processing of personal data, occurring as a result of the embedded third-party plug-in (Question 2); and the potential roles and responsibilities arising as a consequence of such a designation or lack thereof (Questions 3-6).[572]

The extensive deliberations of the Court regarding Question No. 1 are largely irrelevant for the subject of this thesis and will therefore be not be analysed.[573] It should only be noted that the conclusion was reached that Articles 22 and 24 did not preclude the existence of national legislation allowing consumer protection associations to bring or defend legal proceedings against entities responsible for a potential infringement of data protection law.[574] Highly relevant are, however, the deliberations as well as conclusions reached with regards to the role taken by Fashion ID and their respective responsibilities for the processing in question. These are therefore analysed in detail in this thesis.

aa) Role

In its second question, the German Higher Regional Court asked if *"[in] a case such as the present one, in which someone has embedded a programming code in his website which causes the user's browser to request content from a third party and, to this end, transmits personal data to the third party, is the person embedding the content the "controller" within the meaning of Article 2(d) of Directive [95/46] if that person is himself unable to influence this data-processing operation?"*.[575]

The Court of Justice of the European Union started its deliberations by reiterating its previous findings on the subject. It

---

[572]ibid para 42.
[573]For more details see: ibid para 43-62.
[574]ibid para 63.
[575]ibid para 42.

again underlined the fact that the term "controller" was to be interpreted broadly in order to assure a high level of protection of the rights and freedoms of the individual,[576] in particular the effective and complete protection of data subjects.[577] Referring to previous case law on the subject, it clarified that the term was not restricted to a single actor or entity and that a party which *"exerts influence over the processing of personal data, for his own purposes"* may be regarded as such since they would effectively be participating in the determination of the purposes and means of the processing of personal data.[578] Furthermore, the lack of access to personal data does not exclude the possibility of being considered a controller and it is possible for different parties to be involved in different stages of the overall processing activities to varying degrees, since joint liability does not automatically result in equal responsibility.[579]

The CJEU's deliberations also included a reminder on the definition of "processing of personal data" under the Directive, pointing out that such a processing does not need to be limited to one action and can involve a number of operations relating to different stages of the overall processing activity.[580] In that context and taking into account the Opinion of the Advocate General, the court concluded that a party could only be considered a controller for the part of the processing of personal data for which they were involved in the determination of the purposes and means not, however, in any preceding or subsequent operations of the overall chain of processing.[581]

Based on this logic of separately accounting for the different stages of the overall processing activity, the CJEU established that whereas Fashion ID could not be considered a controller for any subsequent processing of personal data conducted by Facebook

---

[576]ibid para 65.
[577]ibid para 66.
[578]ibid para 67f.
[579]ibid para 69f.
[580]ibid para 71f.
[581]ibid para 74.

Ireland after the transmission of the information, they were in fact capable of jointly determining the means and purposes with regards to *"the collection and disclosure by transmission of the personal data of visitors to its website"*.[582] This was based on the fact that Fashion ID had decided to embed the "Like" button in question while being fully aware that it essentially fulfilled the purpose of collecting and transmitting the personal data of individuals who visited the website to Facebook Ireland, regardless of whether they were actually members of their social network.[583] In that sense, the website operator was to be considered as exerting *"decisive influence over the collection and transmission of the personal data"*, since without the inclusion of the plug-in, such a transmission would not have been possible in the first place.[584] Based on this, the court concluded that Facebook Ireland and Fashion ID would need to be considered as jointly determining the means *"at the origin of the operations"*, namely the collection and transmission of the visitor's data.[585] With regards to the purposes, they derived the element of "joint determination" from the fact that the processing of personal data takes place in order to further the economic interest of both parties.[586] In the case of Fashion ID, these interests were realised through a commercial advantage achieved by increasing the publicity of its goods, whereas Facebook would be able to further use the collected information for their own commercial purposes.[587] In the end, the CJEU thereby reached the conclusion that Fashion ID and Facebook were to be considered as joint controllers for the collection and disclosure by transmission of personal data of the users of the website.[588]

---

[582]ibid para 76.
[583]ibid 77.
[584]ibid para 78.
[585]ibid para 79.
[586]ibid para 80.
[587]ibid para 80.
[588]ibid para 84.

bb) Responsibility

Question 3 was deemed irrelevant, since it concerned the possibility of alternative civil liability for processing operations of parties who are not to be considered as "controllers".[589] The same to a certain extent applied to Question 4, as the consent of the website visitors was in principle necessary, based on Article 5(3) of the E-Privacy Directive.[590] The court, however, still decided to deliberate on the issue, concluding that where joint controllers wish to use legitimate interest as their legal basis for the processing of personal data, it is necessary for each of the parties to be pursuing such, in order for the operations to be justified by them.[591]

More relevant, however, in the context of the responsibilities of joint controllers were Questions 5 and 6, which asked for a determination towards whom the data subject would need to declare their consent and who would be responsible for the provision of information regarding the processing activity to such.[592] For those, the Court concluded that since the website operators were to be considered a controller with regards to the collection and transmission of the website visitors' personal data, they would equally be subject to the duty of obtaining their consent and providing information concerning these processing operations.[593] This assumption was also based on practical considerations, since as visiting the operator's website triggers the collection of personal data, they should also be the ones obtaining consent for such, especially since this should be collected prior to the commencement of the processing.[594] The same logic essentially also applied with regards to the duty to inform.[595] These responsibilities would, however, only apply during the processing activity for which the court determined

---

[589]ibid para 86.
[590]ibid para 88.
[591]ibid para 96.
[592]ibid para 42.
[593]ibid para 101.
[594]ibid para 102.
[595]ibid para 104.

joint controllership, namely the initial collection of data and subsequent transmission to Facebook, and not to any further processing conducted by them.[596]

d) Review

The Judgement delivered by the Court in the case of Fashion ID is considered extremely significant in many ways. First of all, it confirmed the previous tendencies of the CJEU in favouring an extensive understanding of joint controllership for the purpose of the assurance of effective and complete protection of the data subject.[597] Secondly, it provided some additional insights on the matters discussed in the previous cases.[598] Most importantly, however, it essentially introduced a new "phase-based approach" by which processing activities may be divided into different stages and joint controllership established only for specific parts.[599] Even more than the previously reviewed cases, *Wirtschaftsakademie* and *Jehovan,* the Court´s findings in *Fashion ID* have been subject to much debate among legal practitioners and academics, including a significant amount of criticism. The following section will thereby provide an overview of the typically voiced points of concern, including some personal opinions.

aa) Alternative or Cumulative Conjuction

A common criticism directed towards the decisions of the Court of Justice of the European Union relates to the previously discussed question as to whether the joint determination of "purposes and

---

[596]ibid para 106.

[597]*Gorkič*, 5 EDPL 2019, 579, 581; *Globocnik*, 50 IIC 2019, 1033, 1036; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 9.

[598]*Paun*, 9 EuCML 2020, 35, 36f; *Gorkič*, 5 EDPL 2019, 579, 581; *Globocnik*, 50 IIC 2019, 1033, 1036; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 40.

[599]*Zalnieriute/Churches*, 83 MLR 2020, 861, 861; https://www.europeanlaw-blog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Becker and others*, 12 IDPL 2022, 207, 212; *Paun*, 9 EuCML 2020, 35, 36f.

means" constitutes an alternative or a cumulative conjunction.[600] As outlined before, both the original Guidance of the Art. 29 WP and the prevailing opinion in literature seem to be in favour of the necessity for the cumulative presence of both elements, while the European Data Protection Board is more vague on the issue. Due to the significant practical relevance of this question, many regret that the CJEU did not take the opportunity to directly address the issue.[601] The tendency does, however, seem to favour the alternative solution by which the joint determination of one of these elements would be sufficient for the establishment of a joint controllership.[602] Such a presumption could, however, result in significant difficulties in differentiating between joint and separate controllers.

bb) Limitation

While this is certainly not one of the most popular points of critique voiced within literature, some sources have taken the position that the judgement put forward an excessive limitation on the scope of joint controllership by only applying it for the collection and transmission of the user's personal data.[603] It is argued that such a limitation does not properly reflect the technical functioning of these plug-ins as well as the purpose of their inclusion onto the website, since the commercial advantage which Fashion ID intended to achieve through the inclusion of such would not be accomplished merely by this part of the processing activity.[604] In order for the "Like" button to properly function and to provide any type of benefit for the website operator, a number of additional processing operations need to be conducted by Facebook.[605] Based on this relation between the

---

[600]See Part 2 Chapter 3: C. II. 3. d) Alternative or Cumulative Conjunction.

[601]*Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 95; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 44.

[602]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 44; *Lee/Cross*, 9 MMR 2019, 559, 561; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720.

[603]*Globocnik*, 50 IIC 2019, 1033, 1037.

[604]ibid.

[605]ibid.

overall processing of the social media provider and the website operator, Fashion ID should have been considered as a joint controller for all elements of the processing of personal data necessary for the proper functioning of the "Like" button embedded onto its website.[606]

cc) Extension

On the other side of the spectrum and definitely brought up more frequently is the opinion that the very broad criteria for the establishment of joint controllership applied by the CJEU essentially led to a boundless expansion of the term, which might now cover almost any sort of involvement in the processing of personal data.[607] As a result, the differentiation between the controllers and processors, or even separate and joint controllers, becomes essentially impossible. In effect, this also leads to a blurring of responsibilities of the respective parties, as well as confusion on the side of the data subject, due to the potential inclusion of too many actors onto the scope of controllership.[608] The Court has defended this extension of the term over scenarios with little to no involvement from one of the parties by repeatedly pointing out that *"joint liability does not necessarily imply equal responsibility"*.[609] This is to a certain extent true, since the parties are left with a great deal of flexibility in defining their respective roles in their required arrangement as per Art. 26. The problem, however, results, not solely from a very flexible and broad understanding of joint controllership, but from combining such with an arguably equally flexible and broad understanding of controller–processor relationships.

---

[606]ibid.

[607]*Finck*, 11 IDPL 2021, 333, 338; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720f; *Lee/Cross*, 9 MMR 2019, 559, 561; *Becker and others*, 12 IDPL 2022, 207, 212; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 42.

[608]*Finck*, 11 IDPL 2021, 333, 338; *Becker and others*, 12 IDPL 2022, 207, 212; *Paun*, 9 EuCML 2020, 35, 36.

[609]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 70; Case C-25/17 *Jehovan* todistajat [2018] ECLI:EU:C:2018:551, para 66.

As has already been established under Part 2 Chapter 3: B. II. 2. b) Margin of Discretion, it is commonly accepted that processors may be granted with a certain margin of discretion when it comes to the selection of the means of the processing of personal data. While generally the purposes of the processing and the determination of essential means are reserved for controllers, processors will still be able to determine many details with regards to the processing activity, especially when it comes to the determination of the technical and organisational measures by themselves. If the definition of processors only included entities acting on explicit instructions of a controller, there would essentially be no issue, since any entity having their own decision-making power would be considered a joint controller, justifying a broad approach to such. Since this, however, is neither how the term is interpreted in literature nor applied in practice, it seems that there is a potentially significant overlap between the different functions. This, in turn, leads to an outcome under which a processor could potentially be more involved in the actual decision-making regarding the technical details of the processing operation than a joint controller with very little responsibilities, making it nearly impossible to differentiate between those.

The dangers of a too far-reaching definition of joint controllership were also pointed out by the Advocate General Michal Bobek in his Opinion, where he warned that the criterion of "making the processing possible" would essentially result in an unlimited number of persons being co-responsible for the processing of personal data, when taking the entire chain of processing into consideration.[610] He also did not agree with the argument that this issue could be solved through a transparent allocation of responsibilities through an arrangement or contract, since such a solution would prove to be unrealistic, taking into account *"the dense web of formal, standard contracts that would have to be signed by any kind of party, including,*

---

[610]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, Opinion of AG Bobek, para 74f.

most likely, a number of normal users".[611] This approach should also not be considered acceptable as it would make the application of legislation and the allocation of responsibility conditional on such agreements.[612]

dd) Broad Purpose

Directly related to criticism of the tendency of unnecessary expansion of the term is the issue of applying a very broad definition of "joint purposes".[613] It is, after all, questionable whether the two entities in question did in fact share a purpose. Fashion ID wished to receive increased publicity for their products, whereas Facebook intended to create personalised ads based on the overall collected data. The CJEU decided to summarise these issues under the common banner of "economic interests".[614] Such a generalisation is, however, inherently unspecific and essentially leads all commercial undertaking to having a common purpose.[615] This broadening also seems extremely unsatisfactory in consideration of the principle of purpose limitation, enshrined in Art. 5(1)(b) of the GDPR, which requires the purposes of the processing of personal data to be *"specified, explicit and legitimate"*. It could therefore be argued that the same requirements would also apply to the joint purposes determined by joint controllers.[616]

This expansion of the extent to which purposes are to be considered as "joint" also again significantly affects the differentiations between joint controllers and processors.[617] As has been outlined under Part 2 Chapter 3: B. II. 2. b) Margin of Discretion

---

[611]ibid para 86.

[612]ibid para 86.

[613]*Lee/Cross*, 9 MMR 2019, 559, 561; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 46; *Hanloser*, 10 ZD 2019, 455, 459.

[614]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 80.

[615]*Golland*, 07 K&R 2018, 433, 436f; *Lee/Cross*, 9 MMR 2019, 559, 561; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 46.

[616]*Specht-Riemenschneider/Schneider*, 2 GRUR Int. 2020, 159, 162.

[617]*Hanloser*, 10 ZD 2019, 455, 459.

above, the determination of the purposes of the processing of personal data is in principle reserved to controllers. This directly relates to the fact that they are also the party obliged to assure the existence of a valid legal basis for the processing operation. It should, however, be noted that processors will also in most instances have their "purpose" in the form of an economic interest of fulfilling the contract and receiving compensation for such. Arguably, this also opens the possibility for those to use Art. 6(1)(b) as a legal basis for the processing of personal data. This purely economic interest in fulfilling one's commissioned contractual obligations for the purpose of compensation has, however, traditionally been considered as falling under the definition of "acting on behalf of" another entity, since there is no underlying further self-interest in the data.[618] If, however, the simple presence of an "economic interest" on the side of both parties amounts to a "joint purpose" this would constitute a significant shift in that approach, again making the differentiation between the different legal figures essentially impossible.

ee) Lack of Factual Influence

With regards to the particular case of Fashion ID, commentators have also voiced some doubt as to the extent to which the website operator is in fact able to extend actual factual influence over the processing of personal data, in this instance.[619] This problem is, in fact, of considerable practical importance since constellations such as these where one large, global conglomerate essentially leaves all potential contracting counterparties with a "take it or leave it" approach, are quite popular in today's economy. The issue also does not only pertain to the question of factual influence but also to the ability of the website operator to provide the data subject with accurate information regarding the processing of Facebook or even gain an accurate understanding of such themselves.[620] In

---

[618] *Sury*, 44 Informatik Spektrum 2021, 376, 376.

[619] Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 45; *Kartheuser/Nabulsi*, 11 MMR 2018, 717, 720; *Finck*, 11 IDPL 2021, 333, 344.

[620] *Schlee*, 14 ZD-Aktuell 2019, 06762; *Finck*, 11 IDPL 2021, 333, 344.

consideration of the relative lack of actual control of the website operator over the action of a large multi-national conglomerate, the publishers have been described as "collateral damage" of an overall trend, by which the supervisory authorities seem to have decided to go after comparatively smaller entities rather than the better resourced corporations, trying to affect the business models of the latter indirectly.[621] Similar observations concerning the lack of actual knowledge or influence over the processing conducted by the contractual counterpart do in fact not only apply in the case of joint controllers, but often in relationships between controllers and processors as well.

Such an "unwillingness" (or inability) to cooperate of one of the involved entities should, however, not lead to a complete exemption from liability of the other counterpart. While website operators might in fact have little or no practical influence over the actions of large social media empires such as Facebook, they do, as accurately pointed out by the CJEU, have a decisive influence in making possible or at least furthering the collection of personal data by such.[622] The lack of collaboration between the parties should, however, also not be without consequence as it precludes the existence of the characteristic of "joint" determination required for the consideration as joint controllers. In that sense, the previous deliberations on the consideration of separate controllership in the context of *Wirtschaftsakademie* should be referred to (see Part 2 Chapter 3: C. III. 1. d) bb) Suggested Solution), as a similar principle could be applied here as well. The establishment of Fashion ID as a controller but separate from Facebook, responsible for the processing of personal data initiated by their website, would still ensure their liability for embedding the plug-in, while not requiring any type of cooperation between the parties or factual influence of the website operator over the social media provider, as the first would simply be responsible for the selection of the latter.

---

[621] *Globocnik*, 50 IIC 2019, 1033, 1042.

[622] Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 75.

ff) Fragmentation

While the very broad criteria used for the determination of joint controllership have led to a significant extension of the term, the CJEU did attempt to limit its boundaries to a certain extent by introducing the concept of joint controllership for specific stages of the processing of personal data. In the case of Fashion ID this was, for example, limited to *"the collection and disclosure by transmission of the personal data of visitors to its website"*, but did not include any prior or subsequent processing of the involved parties.[623] While this limitation might arguably have been introduced in order to avoid the dangers of a too broad responsibility regime pointed out by the Advocate General, as well as those which would inevitably come from other sources, a significant amount of criticism has also been voiced explicitly towards the introduction of this "stage based" approach.[624] First of all, such a "splitting" of the overall chain of processing leads to significant problems in the assurance of transparency and understandability of such for the data subject, as it essentially makes the way in which they will be divided unpredictable and also to a certain extent, obscures the real underlying purpose by artificially limiting it only to a part of the activity.[625] Secondly, the splitting into various stages inevitably leads to a separation of consent notices, which can now be collected for certain fragments of a chain of processing, also creating a hindrance in understanding the overall implications for the affected individual.[626] The data subject might therefore consider a certain element as acceptable and not too invasive, while ignoring or being unable to accurately perceive the

---

[623]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

[624]*Becker and others*, 12 IDPL 2022, 207, 212 *Zalnieriute/Churches*, 83 MLR 2020, 861, 871-875; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Paun*, 9 EuCML 2020, 35, 37.

[625]*Paun*, 9 EuCML 2020, 35, 37; *Zalnieriute/Churches*, 83 MLR 2020, 861, 871-874; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026).

[626]*Zalnieriute/Churches*, 83 MLR 2020, 861, 874.

bigger picture and the risks associated with the connected chain of processing.[627] Also, applying this fragmented approach without a proper framework in place can potentially lead to a number of legal uncertainties with regards to the division of such phases, as well as the roles and responsibilities connected to each of those.[628] The introduction of joint controllership for specific stages of the processing activity is therefore the cause of a large amount of uncertainty in that regard, arguably hindering the completed and effective protection of the individual, rather than furthering it.[629]

4. Intermin Conclusions: Case Law of the Court of Justice of the European Union

In analysing the Case Law of the CJEU concerning the legal figure of joint controllership, a clear tendency of expanding that term has been evidenced. While the legal definition formally required is for two or more controllers to determine the means and purposes of the processing of personal data jointly, the Court has extended the applicability of this terminology to instances in which processing is "made possible" by a party. Elements of cooperation, common purposes, and actual factual influence have largely been derived based on very dubious and seemingly forced argumentation. This has also led to significant criticism from legal practitioners, as well as academic literature.

The reason for which the CJEU seems to be forcefully defining certain legal entities as (joint) controllers self-admittedly lies in the assurance of the "complete and effective" protection of the data

---

[627] *Paun*, 9 EuCML 2020, 35, 37; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Gorkič*, 5 EDPL 2019, 579, 582.

[628] https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 96.

[629] *Paun*, 9 EuCML 2020, 35, 37; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026).

subjects. The reason apparently is rooted in a fear that certain parties which facilitate, support, or make possible the collection (or other processing) of personal data, would otherwise not be legally liable and responsible, based on their limited impact of the overall circumstances. This approach of a gradual broadening of the term has, however, led to a now potentially infinite amount of (joint) controllers being responsible for every single processing operation. The CJEU attempted a limitation of this seemingly boundless liability regime by introducing a "stage-based-approach" by which joint controllership could be assumed by two or more entities for certain stages of the processing, leaving out any previous or subsequent actions. This, however, arguably has raised more problems than it actually solved by potentially making processing operations involving more than one party even less transparent, as well as introducing a number of legal uncertainties with regards to the consequences of such a division.

While the motives of the Court of Justice of the European Union are both admirable and understandable, it seems that the effect of the currently applied definition of joint controllers has the potential to cause more harm than good. This is quite unfortunate as it would seem that the introduction of such a confusion was largely unnecessary for the assurance of the complete and effective protection of the individual's rights, as originally intended. In the view presented here, the same goal could have been reached through the simple assumption of separate controllership, rather than joint. Instead of separating the chain of processing into different stages, it should have simply been separated into individual processing activities, conducted by separate individual controllers. In the case of *Wirtschaftakademie*, this would have been the administration of a Facebook fan page and, in the case of *Fashion ID,* the running of a website which included third-party plug-ins, causing a transfer of personal data to another controller. In both instances, the simple assumption of a separate controllership in which the controller is responsible for the selected means of processing, including decisions made on the involvement of certain social media channels, would be entirely sufficient to assure that there is no gap in the

protection of the rights of the individual, without introducing a convoluted reasoning as to why two entities which do not make any joint determination on the means or purposes of the processing of personal data, should be considered joint controllers.

Regardless of any voiced criticism and personal opinions, the definitions, considerations, and relevant factors for joint controllership introduced by the case law of the CJEU are what is ultimately relevant for the determination of joint controllership for the purpose of this thesis, and should therefore be applied accordingly.

IV. Effect

As has been the case with the previously described roles of controllers and processors, the designation as a joint controller will result both in multiple obligations, as well as entail a number of serious consequences for the party, all of which will be discussed in this section.

1. Responsibilities

Where two or more entities determine the means and purposes of the processing of personal data jointly, a number of obligations will arise as a result of engaging in such a relationship. The central Article regulating the instances of joint controllership in that regard is Art. 26, since the involved parties, however, also fall under the definition of controller under Art. 4 No. 7 and the general obligations applying to such will also require consideration. The details of the interplay of Art. 26 and the general responsibilities of the controller, as well as consequences resulting from joint authority over the processing activity, will therefore be outlined below.

a) Contract

Article 26(1) introduces the requirement for joint controllers to determine their respective responsibilities and duties by means of an arrangement, unless these have already been determined by Union or Member State law.

aa) Form

In contrast to the requirements for contracts between controllers and processors put forward in Art. 28(9), Art. 26 does not demand a specific form for the arrangement concluded between multiple controllers.[630] The Article does, however, contain a number of stipulations which would need to be considered in the context of determining the form of such an agreement. First of all, Art. 26(1) provides that it should be concluded in a transparent manner. The purpose of this requirement can, on the one hand, be understood as facilitating a clear division of responsibilities for the involved parties but also likely serves the purpose of allowing the supervisory authorities to efficiently make use of their investigative powers.[631] Secondly, in accordance with Art. 26(2), the essential content of such should also be made available to the data subject, which means that the provided information will also need to be concise, easily accessible, and easy to understand using clear and plain language, as outlined in Recital 58 and previously discussed in the context of the right to information (see Part 1 Chapter 2: B. I. 1. Form).[632] Furthermore, as a result of the principle of accountability, the parties will be required to be able to demonstrate their compliance with the prerequisites of Art. 26.[633] In the same vein, the respective responsibilities would also need to be included in the record of processing activities in accordance with Art. 30.[634] Taking into account these factors, it can therefore be assumed that while there is no explicit obligation for the parties to put

---

[630]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 52; Eßer/Kramer/von Lewinski / *Schreibauer*, Art. 26 DSGVO, para 16; *Lezzi/Oberlin*, 9 ZD 2018, 398, 402; Kuner and others / *Millard/Kamarinou*, Art. 26, 582, 587.

[631]*Lezzi/Oberlin*, 9 ZD 2018, 398, 402; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 52.

[632]*Specht-Riemenschneider/Schneider*, 8 MMR 2019, 503, 505; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 52.

[633]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 52; Eßer/Kramer/von Lewinski / *Schreibauer*, Art. 26 DSGVO, para 17.

[634]Kuner and others / *Millard/Kamarinou*, Art. 26, 582, 587.

their arrangement in written form, it will in practice, be necessary to create some sort of written documentation for the contents of such.[635]

bb) Content

Whereas the stipulations for the content of the arrangement between the parties are again far less explicit than in the case of commissioned data processing under Art. 28, there are still a number of elements which the parties are legally required to determine in advance in order to assure the protection of the individual's personal data.

(1) Allocation of General Responsibilites

As per Art. 26(1), the parties need to determine their respective responsibilities for compliance with the obligations under GDPR. In that sense, the primary goal constitutes the accurate allocation of responsibilities in order to facilitate the complete and effective protection of personal data.[636] As already outlined under Part 2 Chapter 3: A. VI. 1. Responsibility previously, the Regulation essentially establishes the controllers as the central figure responsible for the assurance of the protection of personal data by outlining a number of duties for such through the entire text. While listing each and every one of them would be excessive and largely derivative, examples include, however, obligations such as: guaranteeing the main principles of data protection (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability); the maintenance of a record of processing activities and of necessary measures for the

---

[635]*EDPB*, Guidelines 07/2020, para 171; Kuner and others / *Millard/Kamarinou*, Art. 26, 582, 587; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 52; Eßer/Kramer/von Lewinski / *Schreibauer*, Art. 26 DSGVO, para 17; *Lezzi/Oberlin*, 9 ZD 2018, 398, 402; *Specht-Riemenschneider/Schneider*, 8 MMR 2019, 503, 505.

[636]*Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 91; Kuner and others / *Millard/Kamarinou*, Art. 26, 582, 587; Gola/Heckmann / *Piltz*, Art. 26 DSGVO, para 2.

security of personal data; as well as the performance of data protection impact assessments and the reporting of breaches, where necessary.

While the wording in Art. 26(1) suggests that these responsibilities can be divided freely it is, however, to a certain extent questionable whether all of these can be delegated or whether some would need to be provided for by each of the involved parties.[637] Handing over tasks such as the notification of personal data breaches to the supervisory authorities, the communication of such to the data subject, the performance of a data protection impact assessment, or the assurance of certain specific technical and organisation security measures to one of the parties, seems largely unproblematic.[638] The allocation of these should not be random and take into account the competence of the parties in that regard, as well as their influence over the processing of personal data.[639] A free division of more central duties such as the assurance of the principles of data protection, enshrined in Art. 5, or the provision of a legal basis for the processing activity, is however at least questionable.[640]

The Guidance of the EDPB is unfortunately somewhat unclear in that regard. On the one hand, the implementation of general data protection principles—the legal basis for processing, security measures, the notification of breaches, Data Protection Impact Assessments, the use of processors, data transfers to third countries, and the organisation of contact with data subjects and supervisory authorities—are all listed as responsibilities, which may be determined within the agreement between the parties.[641] On the other hand, the Board makes clear that each controller has the duty to ensure a legal basis and that data is not further processed for purposes

---

[637] *Lezzi/Oberlin*, 9 ZD 2018, 398, 402.

[638] Eßer/Kramer/von Lewinski / *Schreibauer*, Art. 26 DSGVO, para 14; *Lezzi/Oberlin*, 9 ZD 2018, 398, 402.

[639] *EDPB*, Guidelines 07/2020, para 165.

[640] *Lezzi/Oberlin*, 9 ZD 2018, 398, 402.

[641] *EDPB*, Guidelines 07/2020, para 163.

incompatible with those identified at the time of collection.[642] Also, requirements unrelated to the joint processing but generally resulting from their roles as a controller, such as the maintenance of a record of processing activities and the designation of a DPO, seem to be excluded from distribution.[643] The EDPB clarifies in that context that the extent to which the respective responsibilities may be disseminated between the parties, would depend on *"the nature and context of the joint processing"*.[644] Controllers are therefore still generally advised to monitor compliance with all duties resulting from the GDPR, unless those clearly fall outside of the scope of their involvement in the processing activity. It should, however, be noted that even where the transfer of a certain responsibility might be deemed invalid by the DPA, the possibility of indemnification for the incurred damages could still be available, potentially making such a designation quite relevant.

(2) Allocation of Responsibilities with Respect to the Exercise of Data Subject Rights

Additionally, to obliging the parties to determine their respective responsibilities for compliance with their duties under the GDPR in general, Article 26(1) further specified that this should concern the exercising of the data subject's rights and the right to information, in particular. While this clarification does not in principle add any new requirements with regard to the content of the agreement, as the assurance of data subjects' rights are either way part of the controller's responsibilities, it does underline the importance attributed to this aspect by the lawmakers. This element in a sense highlights the main goal, which is the protection of the data subject and their interests by reminding the parties that it is crucial for them to consider all rights available to the individual in advance and make sure that these are

---

[642]ibid para 164.
[643]ibid para 168.
[644]ibid para 167.

all complied with.[645] The emphasis on these particular responsibilities is also justified considering that the consequences of an inaccurate or unclear distribution would in this case be borne by an individual who is not a party to the agreement. After all, where controllers fail to transparently assign their respective tasks in other contexts, they are likely to be exposed to the most serious ramifications. In the context of data subject rights, however, any type of imprecision or uncertainty might inadvertently affect the data subject directly. This notion is also further supported by Art. 26(2), which provides that the arrangement *"shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects*".[646]

(3) Designation of a Contact Points

In line with the general focus on assuring that the presence of joint controllership and the effect of such on the processing of personal data is understandable for the data subject, Art. 26(1) further provides that the parties may designate a contact point for data subjects in their arrangement. While there is no requirement to do so, the European Data Protection Board does generally recommend it.[647] The designation of such a point is, after all, considered to support more transparency for individuals through providing them with a clear contact in case of questions regarding the processing of their personal data, while also facilitating efficient coordination between the joint controllers.[648] The designation of such is, however, primarily to be considered as a form of "service offering" for the data subject and does not bear any additional legal consequences.[649]

---

[645]ibid para 175.

[646]*Radtke*, Gemeinsame Verantwortlichkeit, 251.

[647]*EDPB*, Guidelines 07/2020, para 181f.

[648]*EDPB*, Guidelines 07/2020, para 181f; Eßer/Kramer/von Lewinski / *Schreibauer*, Art. 26 DSGVO, para 16.

[649]Paal/Pauly / *Martini*, Art. 26 DSGVO, para 29; *Specht-Riemenschneider/Schneider*, 8 MMR 2019, 503, 506; *Lezzi/Oberlin*, 9 ZD 2018, 398, 402.

(4) Other Aspects

The listing of responsibilities to be allocated under Art. 26 is non-exhaustive and joint controllers are generally free to outline additional details of their relationship within such an agreement.[650] Sources in literature *often* suggest the analogous inclusion of aspects listed in Art. 28(3) such as, for example, the subject matter and duration of the processing, its nature and purpose, the type of personal data being processed, and the categories of data subjects affected by such.[651] Also advisable in that regard may be the inclusion of a detailed overview of the specific phases of the processing activity, as well as the respective parties involved in such.[652] This should also cover the modalities of the future termination of the processing and a corresponding exit strategy.[653] Other details, such as rules for engaging processors or other parties, the performance of Data Protection Impact Assessments, or rules governing data transfers to third countries could, for example, also be added where necessary.[654]

cc) Availability

Article 26 does not only regulate the content and form of the arrangement between joint controllers, but sets out stipulations for its availability as well. Namely, Paragraph 2 therein provides that the *"essence of the arrangement shall be made available to the data*

---

[650] *EDPB*, Guidelines 07/2020, para 162; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 59; *Specht-Riemenschneider/Schneider*, 8 MMR 2019, 503 505; *Schreiber*, 2 ZD 2019, 55, 56.

[651] *Schreiber*, 2 ZD 2019, 55, 57; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 59.

[652] *Lezzi/Oberlin*, 9 ZD 2018, 398, 402; *Schreiber*, 2 ZD 2019, 55, 57; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 55.

[653] *Specht-Riemenschneider/Schneider*, 8 MMR 2019, 503, 506; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 59.

[654] *EDPB*, Guidelines 07/2020, para 163; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 59; *Schreiber*, 2 ZD 2019, 55, 57.

subject". This is necessary for the data subject to gain an understanding of the processing activities and the respective roles taken by the involved parties with regard to such and closely relates to the general principle of transparency, enshrined in Art. 5(1)(a) of the GDPR.[655] Opinions on what in fact constitutes *"the essence"* of the agreement vary. Some sources only include the legally required terms of the agreement under that definition,[656] whereas others seem to support the notion that all the elements listed in Articles 13 and 14 should be covered.[657] From a practical perspective this dispute is, however, largely irrelevant since, regardless of which points exactly are to be considered as *"essential"* in the meaning of Art. 26(2), the parties would either way be required to provide that information in accordance with Art. 12(1).

While the extent of the specific information which needs to be provided to the data subject is arguable, there seems to be a general consensus with regard to the second relevant element of this stipulation: the *"making available"*. Here sources agree that no active communication is required from the controllers in that context; rather simply assuring that the relevant information can be accessed by the individual should be considered sufficient.[658] There are also no specifications with regards to the form in which availability should be assured, in principle allowing the parties to freely select the most effective way taking into account the context of the processing, as well as the interest of the data subject.[659] The most convenient and fre-

---

[655] *EDPB*, Guidelines 07/2020, para 177; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 26; *Lezzi/Oberlin*, 9 ZD 2018, 398, 403.

[656] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 26; *DSK*, Kurzpapier Nr. 16, 4; *Lezzi/Oberlin*, 9 ZD 2018, 398, 402.

[657] *EDPB*, Guidelines 07/2020, para 171; Kuner and others / *Millard/Kamarinou*, Art. 26, 582, 587; *EDPB*, Guidelines 07/2020, para 179.

[658] *Lezzi/Oberlin*, 9 ZD 2018, 398, 403; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 27; Paal/Pauly / *Martini*, Art. 26 DSGVO, para 35.

[659] *EDPB*, Guidelines 07/2020, para 179.

quently used forms in that regard are likely the inclusion of the relevant details as part of the privacy policy, notifications under Art. 13 or 14, and as part of the website.[660]

b) Data Subject Rights

An important aspect concerning the responsibilities of joint controllers is contained in Art. 26(3), which provides that data subjects may exercise their rights under the GDPR against each controller, irrespective of the responsibilities and terms agreed upon between the parties in the previously mentioned arrangement. This essentially means that even where the contract between the joint controllers clearly designates the responsibility for providing a certain data subject right to one party, the data subject may still demand accommodation from any of the other entities.[661] The reason for the inclusion of such a stipulation clearly lies in the protection of the individual whose data is being processed. It essentially assures the data subject that they are not incurring any risks from potentially unclear terms agreed upon by the parties, or complicated company and processing structures.[662] Controllers should thereby be prohibited from referring individuals to other legal entities; rather the issue must be solved internally between each other.[663] After all, being delegated from one contact point to another would constitute a significant burden for such an individual and could effectively hinder them in the exercise of their right.[664] This can be particularly relevant in the case of international data transfers where one controller might be located in the country of residence of the data subject, whereas others might

---

[660]*EDPB*, Guidelines 07/2020, para 179; *Lezzi/Oberlin*, 9 ZD 2018, 398, 403; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 27; Paal/Pauly / *Martini*, Art. 26 DSGVO, para 35.

[661]*EDPB*, Guidelines 07/2020, para 186; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 28.

[662]Paal/Pauly / *Martini*, Art. 26 DSGVO, para 36.

[663]*Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 28; Paal/Pauly / *Martini*, Art. 26 DSGVO, para 36.

[664]*EDPB*, Guidelines 07/2020, para 187.

be established in other Member States or even outside of the European Economic Area.[665]

c) General Obligations

While Article 26 constitutes the central norm governing the legal figure of joint controllership, general obligations regulating the roles and responsibilities of these parties can be found throughout the entire text of the GDPR. Since joint controllers are in a sense a subtype of controllers and do not constitute a completely separate function, as was the case with processors, all of the responsibilities and requirements set out by the Regulation for controllers in general will essentially apply for joint controllers as well.[666] These can, however, to a certain extent be limited by means of the arrangement between the joint controllers, which will set out their duties in accordance with Art. 26(1). In that sense, where a certain obligation is transferred to one of the other joint controllers as part of the contract between them, an entity might be relieved from such. This possibility, however, is again limited by the previously analysed Art. 26(3), which essentially hinders the transfer of such obligations with respect to the data subjects' rights. Also, as discussed under Part 2 Chapter 3: C. IV. 1. a) bb) (1) Allocation of General Responsibilities, limitations on the types of duties which might be shifted onto the counterparties might also be limited based on the practical factual circumstances of the processing activity or on their essential connection to a controller.

As is evidenced by the above considerations, the determination of the actual obligations for a specific joint controller can constitute a quite daunting task and is likely to involve many legal uncertainties with regard to the actual validity of the assignment of some duties. While therefore, the figure of joint controllership technically allows for responsibilities to be shared, promising potential relief to the involved entities, each of the parties will likely still have to assure all of the important guarantees for processing of personal data, within their

---

[665] *EDPB*, Guidelines 07/2020, para 185.

[666] For details on those Chapter 3. A. VI. 1. Responsibility can be referred to.

own right. As a result, in many instances the involvement of other parties will therefore likely cause additional risks, rather than mitigate the existing ones, at least when it comes to the actual handling of the data in question. There are, on the other hand, quite substantial benefits which might potentially arise for joint controllers with regards to the liability for the processing operation, which shall be discussed in the following text.

d) Obligations toward the Data Subject Authorities

In their Guidelines on the concept of controller and processor, the European Data Protection Board also states that joint controllers should establish within their arrangement required under Art. 26, the way in which they intend to communicate with the Data Protection Authorities.[667] Such a communication will typically be necessary in the context of consultations relating to the performance of a Data Protection Impact Assessment, the designation of a Data Protection Officer, or the notification of a personal data breach.[668] Communication with the DPA might, for example, also be necessary in connection with the approval of codes of conduct, certifications, and binding corporate rules (Art. 58(3)(d), (f) and (j)), as well as general advice concerning the controllers' duties, as part of the DPA's advisory powers.

While Art. 26 does not formally require the form or terms of communication with the DPA to be regulated within the contract between joint controllers, it is certainly advisable, considering not only the importance of the subject but also potential risks and varying approaches of the parties towards it. While some may be proponents of an ongoing active communication with their respective supervisory authority, others may take a more conservative approach and prefer to limit such consultations to a minimum, in order to avoid overly exposing themselves. It should also be noted that while the EDPB es-

---

[667] *EDPB*, Guidelines 07/2020, para 188.
[668] ibid para 188.

tablishes that the parties should regulate the modalities of communication among each other, it also points out that the effect of such an arrangement is only internal and that the data protection authorities are in no way bound by these terms.[669] This includes the designation as joint controllers and the provided contact point.[670] In that sense, the DPAs will still be able to exercise all of their powers as outlined under Article 58, regardless of any contractual agreements between the parties.[671]

2. Consequences

Once the obligations resulting from joint controllership are established, the potential consequences for failing to meet these should be analysed. In the same form as shown previously in the context of singular controllers and processors, these can broadly be divided into measures imposed by the Data Protection Authorities or direct liability for suffered damages towards individuals.

a) Powers of Data Protection Authorities

The term “joint controllers” is not mentioned in Article 58 at all. This, however, clearly does not indicate that supervisory authorities cannot exercise any powers against such. Since, however, joint controllers are also to be considered as controllers under Art. 4 No. 5, naturally all of the powers of the DPA, which might be directed against such, will equally apply where two or more are determining the means and purposes of the processing of personal data jointly. In that sense, Chapter 3: A. VI. 2. a) Powers of the Data Protection Authorities can largely be referred to for details on such. Also, as has already been mentioned before, they are not bound by any arrangements made between the parties as part of their contract under Art. 26 or otherwise, meaning that all powers can be exercised to their

---

[669]ibid para 189.
[670]ibid para 189.
[671]ibid para 189.

full extent directly against any of the joint controllers.[672] In that sense, the efficient performance of the supervisory authorities' tasks is to a certain extent simplified in the context of joint controllership, since they are able to freely choose which controller to pursue.

aa) Imposition of Fines

While all of the investigative, corrective, and authorisation powers in principle affect single, separate, and joint controllers equally, there might be very slight variations when it comes to the imposition of administrative fines under Art. 83. First of all, where joint controllers fail to determine their respective responsibilities for compliance with the obligations under this Regulation, as required by Article 26, this infringement can result in the imposition of an administrative fines under Art. 83(4)(a), which may constitute up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year.[673] This could occur based on any violation of Art. 26 such as: (1) failing to conclude an arrangement at all; (2) concluding an arrangement which does not meet the minimum content requirements outlined by the provision; (3) acting against the stipulations of this arrangement; or (4) failing to make the essence of the agreement available to the data subject.[674] Such fines would, however, not be subject to joint and several liability but rather should be established separately for each (joint) controller, in accordance with the criteria set out in Art. 83(2).[675]

bb) Limitation of Fines

Fines can be imposed for any infringements of the Regulation outlined in Art. 83(4) and (5). As already mentioned, these are also not

---

[672]ibid para 189.

[673]*Berger/Eisendle*, 15 IJLT 2019, 20, 38; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 66; Taeger/Gabel / *Lang*, Art. 26 DS-GVO, para 119.

[674]*DSK*, Kurzpapier Nr. 16, 4; Taeger/Gabel / *Lang*, Art. 26 DS-GVO, para 119; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 26' DSGVO, para 47.

[675]Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 26' DSGVO, para 48; Taeger/Gabel / *Moos/Schefzig*, Art. 83 DS-GVO, para 119.

subject to joint and several liability, as is the case with damages awarded under Art. 82, meaning that their amount should be administered in consideration of each individual case, as required by Art. 83(2).[676] The existence of a contract outlining the respective responsibilities for compliance with the obligations under this Regulation of each of the involved parties does, however, raise the question to what extent the supervisory authorities can and should take into consideration the content of such, when deciding upon the imposition of a fine.[677]

While the content of the agreement is not binding for the authorities and Art. 83(2) does not include anything about the responsibility of joint controllers or the divisions thereof in accordance with Art. 26, it would seem possible and certainly fair to take this element into consideration as well, especially if one of the parties had a reasonable expectation that certain obligations would be assured by the other (joint) controller. An example of this includes certain duties which very clearly cannot be shifted onto another actor because of an explicit legal limitation. Due to practical factual circumstances of the processing activity or based their essential connection to a controller, these would generally be excluded from the scope.[678] For all other obligations which might be easily divided amongst parties, the consideration of this element when determining to what extent a fine should be imposed does seem possible.[679] This should in particular apply where specific technical and organisational measures have been delegated to one of the parties, considering that Art. 83(2)(d) does include *"the degree of responsibility of the controller or proces-*

---

[676]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 66; Schwartmann/Jaspers/Thüsing/Kugelmann / *Kremer,* 'Art. 26' DSGVO, para 48; Taeger/Gabel / *Moos/Schefzig*, Art. 83 DS-GVO, para 119.

[677]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 66.

[678]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 66; Eßer/Kramer/von Lewinski / *Schreibauer*, Art. 26 DSGVO, para 14; *Lezzi/Oberlin*, 9 ZD 2018, 398, 402.

[679]Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 66; *Monreal*, 12 ZD 2014, 611, 612.

sor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32" into the scope of factors, to which due regard should be given. Since, however, there is no actual obligation for the supervisory authority to take the content of the agreement under Art. 26 into account, joint controllers are generally advised to include provisions regulating the possibility of indemnification for fines into such.[680]

b) Liability

As was the case with Articles 58 and 83, the ramifications of which have been analysed earlier in this text, the term "joint controllers" is not explicitly mentioned in Art. 82. The rules governing the liability of such will therefore largely be identical to those applicable to single controllers. Still, there are some crucial implications arising from the inclusion of two or more parties into the scope of authority over the processing of personal data, which will shall be analysed in the following passages.

aa) Eligibility and Damages

In accordance with Art. 82(1), the right to receive compensation for their suffered damages can be asserted by any person who has suffered material or non-material damage as a consequence of an infringement of the GDPR. Since the amount of parties involved in the processing of personal data and their respective responsibilities have no bearing on defining the scope of individuals entitled to a claim or the extent of the damages which need to be considered, the already presented analysis of Art. 82(1) under Part 2 Chapter 3: A. VI. 2. b) aa) Eligibility and A. VI. 2. b) aa) Damages can be referred to in that regard.

bb) Infringement and Causation

While the term "joint controllers" is not explicitly mentioned, Article 82(2) does clearly refer to instances where multiple controllers might

---

[680]Taeger/Gabel / *Moos/Schefzig*, Art. 83 DS-GVO, para 119.

be involved in the processing of personal data since it states that *"any controller involved in the processing"* should be held liable for the damages arising as a result of a processing of personal data which infringes the Regulation. There must, therefore, be an infringement of the Regulation (see more on the term under Part 2 Chapter 3: A. VI. 2. b) cc) Infringement of the Regulation), as well as a causal link between such and the established damages.[681] Based on the CJEU's practice in the context of civil liability for violations of competition rules it can be assumed that a *"causal relationship"* between the harm and the prohibited practice will be necessary.[682]

It is, however, important to note that the Regulation does not in fact require a causal link between the controller's actions and the occurrence of the infringement or the damages. In order to give rise to a claim for damages, it is sufficient to determine that a processing activity was in breach of the requirements under the GDPR without having to actually prove any direct fault of misconduct on the controller's side.[683] In cases where a single controller is responsible for the processing of personal data, this outcome quite logically follows from the way in which the GDPR establishes the controller as the central figure responsible for the assurance that processing is being conducted in compliance with the requirements of data protection law, thereby assuming that even if was not the actions of the controller that led to the infringement, there is at least presumably an omission on their side.

Due to the wording in Art. 82(2) establishing liability for *"any controllers involved"*, the same assumption is, however, also transferred onto all of the entities which have jointly determined the means and

---

[681]Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1175; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 41; Paal/Pauly / *Frenzel*, Art. 82 DSGVO, para 11; *Cordeiro*, 5 EDPL 2019, 492, 495.

[682]Joined cases C-295/04 to C-298/04 *Vincenzo Manfredi and Others* [2006] ECLI:EU:C:2006:461, para 61; Case C-199/11 *Europese Gemeenschap* [2012] ECLI:EU:C:2012:684, para 43; Case C-557/12 *Kone AG and Others* [2014] ECLI:EU:C:2014:45, para 22.

[683]*Cordeiro*, 5 EDPL 2019, 492, 497; *Paal*, 1 MMR 2020, 14, 15; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 23.

purposes of the processing of personal data.[684] The term "involved" is quite wide, especially considering that as per Art. 4 No. 2 processing includes both single operations and sets thereof. In that sense, the engagement at any step of the processing would already potentially trigger liability under the GDPR, no matter how small.[685] This also means that any time a processing operation infringes data protection law, any of the (joint) controllers will be potentially liable for the consequences, regardless of their actual fault in the causation of such or the responsibilities outlined in the agreement under Art. 26.

cc) Exemption

This very extensive scope of liability of (joint) controllers regardless of the actual extent to which such involvement occurs and of the agreed upon roles and responsibilities of the parties, does naturally raise the question under which modalities an exemption from such might be possible. As per Art. 82(3), controllers and processors can be exempt from liability if they are able to prove that they are *"not in any way responsible for the event giving rise to the damage"*. As has been established before, the selection of the wording *"not in any way"* indicates a very narrow understanding of this term, meaning that even the slightest level of negligence on the side of the controller will exclude the applicability of such.[686] Typical examples of instances where this might apply in the case of single controllership include unlawful acts by other parties, a lack of fault on the side of the controller, or *force majeure* (see Part 2 Chapter 3: A. VI. 2. b) ff) Exemption).

---

[684]Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1176; *Cordeiro*, 5 EDPL 2019, 492 497; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 22.

[685]Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 22; Paal/Pauly / *Frenzel*, Art. 82 DSGVO, para 13; *Paal*, 1 MMR 2020, 14, 15.

[686]Schwartmann/Jaspers/Thüsing/Kugelmann / *Schwartmann/Keppeler/Jacquemain,* 'Art. 82' DSGVO, para 33 Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 54; *Geissler/Ströbel*, 47 NJW 2019, 3414, 3415; *Paal*, 1 MMR 2020, 14, 17; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204.

Especially relevant, however, in the context of joint controllers is the question whether the terms of the arrangement concluded between the parties in accordance with Art. 26 could be used in order to prove a lack of responsibility. This could, for example, be the case where the contract clearly states a duty to provide certain guarantees or security measures for one party, which failed then to do so. If the lack thereof were to lead to the occurrence of damages for the data subject, all controllers involved at any stage of the processing of personal data would potentially be liable under Art. 82(2), but arguably *"not responsible"* or *"in no way responsible"* for the occurrence of the damaging event, since there was a reasonable expectation that the necessary measures would be assured by their contractual counterpart.

As has been previously established, there is some debate regarding the possibility of exculpation for the misconduct of processors acting outside of or contrary to the received mandate and while some sources are in fact in favour of this approach, most arguments point against accepting such.[687] Many of the voiced arguments, in particular those concerning the central importance of assuring effective compensation for the data subject and thereby only limiting the scope of the parties against which damages can be claimed to the extent that this is absolutely necessary, also apply here. Most importantly, however, exculpation based on the division of responsibilities between the parties will largely be precluded based on the stipulations of Art. 26 (3), which provides that the data subject may exercise their rights against each of the controllers, irrespective of the terms of the arrangement.[688] While one might initially be inclined to primarily think about the data subject right outlined in Chapter III within the Articles 15-22 of the GDPR, Art. 26(3) does not indicate a limitation to such,

---

[687]For more details on the overall debate and all of the relevant factors refer to Part 2 Chapter 3: A. VI. 2. b) ff) Exemption.

[688]Paal/Pauly / *Martini*, Art. 26 DSGVO, para 36; Kühling/Buchner / *Hartung*, Art. 26 DSGVO, para 63; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 26 DSGVO, para 28-29.

meaning that its stipulations should equally apply to the right to compensation and liability enshrined in Art. 82.

dd) Joint and Several Liability

As outlined in the context of the liability of processors, the Art. 82(4) establishes a regime of joint and several liability for instances where multiple parties are involved in the processing of personal data stating that any such (joint) controller or processor should be *"held liable for the entire damage"*.[689] Thereby where two or more entities are determining the means and the purposes of processing of personal data, the data subject is free to select from whom to claim damages.[690] Awarding damages based on the actual responsibility of each controller is, however, possible where the joint controllers are also joined to the same judicial proceedings and full and effective compensation of the individual is still ensured (Recital 146). In such instances, the terms of the arrangement between the parties might in fact gain significance since they would allow the court to determine how the joint controllers have divided their duties amongst themselves, potentially indicating who should be held accountable for the infringement causing the damages.

ee) Indemnification

Whether or not proceedings against multiple controllers would in fact be joined will ultimately depend on the preference of the claimant, as well as the procedural regulations of the respective Member States. As of the time of writing, these instances of applying proportional liability seemed to be of little practical relevance.[691] It is therefore still likely that a joint controller will be forced to compensate a

---

[689]Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1176; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204; *Paal*, 1 MMR 2020, 14, 18; *Kohn*, 11 ZD 2019, 498; 501; Ehmann/Selmayr / *Nemitz*, Art. 82, para 58; Rücker/Kugler, *Schumacher*, D. General conditions, para 831.

[690]*Wybitul/Leibold*, 4 ZD 2022, 207, 209; *Van Alsenoy*, 7 JIPITEC 2016, 271, 285; Kühling/Buchner / *Bergt*, Art. 82 DSGVO, para 57.

[691]Ehmann/Selmayr / *Nemitz*, Art. 82, para 63; *Paal*, 1 MMR 2020, 14, 18f.

data subject directly for the entirety of the damages, even when they might only be partially responsible for the occurrence of such. Should that be the case, they are given the option of indemnification under Art. 82(5) which provides that where a controller or processor has paid full compensation for the claimed damages, they are entitled to claim back part of the compensation from the other controllers or processors corresponding to the level of responsibility each of the parties bears with regards to the infringement and the damages caused by such. This is, therefore, likely the point at which the content of the arrangement between the joint controllers, concluded under Art. 26, will become most relevant as it allows the parties to clearly demonstrate the agreed upon roles and responsibilities with regards to the processing of personal data. This is why joint controllers are generally advised to include more details than formally legally required into their data processing agreements. Ideally, those should also already include an indemnity clause, stipulating how and when a claim for compensation would arise.

V. Interim Conclusions: Joint Controllers

Another crucial scenario under which there are multiple parties involved in the processing of personal data is the legal figure of joint controllership. The two Articles which essentially define this term are Art. 4 No. 7 and Art. 26(1) GDPR. The first establishes the characteristics of a controller, thereby providing a foundation for the definition. The latter specifies under which circumstances the element of “joint” controllership (rather than individual) will occur.

As established under Part 2 Chapter 3: A. Controller, a controller is any natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Should two or more separate legal entities be controllers with regards to a certain processing activity, the applicability of Art. 26 can be considered. Article. 26(1) stipulates that two or more controllers will be regarded as joint controllers where they jointly determine the purposes and means of processing. As a result, the decision-making power over the processing of personal data must be present for two separate

entities at the same time, with both of those entities realising this authority together. A joint determination of purposes requires both controllers to conduct the processing for the same reasons, thereby attempting to achieve compatible or common goals; the extent to which needs to be determined jointly may vary. Parties are free to divide the various elements of the processing operations between themselves. Essential for the applicability of Art. 26 is, however, the "joint" determination of these aspects, meaning that there needs to be some sort of communication between the parties. Simply performing the same type of processing for the same purpose next to each other without any agreement, will therefore not suffice for the applicability of Art. 26. Here the controllership will likely be separate, rather than joint.

The legal figure of joint controllership has gained much prominence over the last years, not only by its more explicit inclusion in the GDPR through Article 26 but also as a result of the case law of the Court of Justice of the European Union. The three landmark rulings concerning this form of cooperation in the context of processing personal data, *Wirtschaftsakademie Schleswig-Holstein*, *Jehovan todistajat* and *Fashion ID*, are detailed in this thesis. The findings therein have been subject to significant attention from both practitioners and academia, as well as a heated debate concerning the further consequences and implications of the standards established by the Court.

In the *Wirtschaftsakademie* case, the court established that the administrator of a Facebook fan page was to be considered as a joint controller with the network itself, based on the fact they have the possibility of defining certain parameters for the page and that they are providing Facebook with the opportunity to collect cookies. *Jehovan todistajat* was concerned with the door-to-door preaching activities of the Jehovah's Witness community. Here the court concluded that these do not fall under household exemption and that while the individual members of the community freely determine which information to gather and how to utilise it in the future, the overall purpose of the entire process lies in supporting the objectives of the Jehovah's Witness community as a whole, thereby making the

community and its members joint controllers. The final and arguably most important ruling, *Fashion ID*, concerned a website operator that had embedded a "Like" button onto their page which was transmitting the users' personal data to Facebook. Here joined controllership of both parties was again confirmed based on the goal of "effective and complete" protection of natural persons; the extent of it was, however, limited to the collection and disclosure by transmission of the data and any subsequent processing conducted by Facebook explicitly excluded from the scope.

The general tendency of the CJEU to gradually expand the definition of joint controllership has led to significant criticism from legal practitioners as well as academic literature. While the legal definition formally requires for two or more controllers to determine the means and purposes of the processing of personal data jointly, the Court has extended the applicability of this figure to instances in which processing is "made possible" by a party, basing elements of cooperation, common purposes, and actual factual influence on a very dubious and seemingly forced argumentation. The reason given for the extension of the terminology is the assurance of complete and effective protection of the individual as otherwise this would seemingly leave them without the necessary legal guarantees. This thesis argues, however, that the same goal could have been reached through the simple assumption of separate controllership, rather than joint.

Where two or more entities determine the means and purposes of the processing of personal data jointly, a number of obligations will arise as a result of engaging in such a relationship. First of all, Article 26(1) introduces the requirement for joint controllers to determine their respective responsibilities and duties by means of an arrangement, unless these have already been determined by Union or Member State law. While there is no explicit obligation for the parties to put their arrangement in written form, it will in practice be necessary to create some sort of written documentation of the contents of such. With regards to the content, the parties are legally required to allocate their respective responsibilities as controllers amongst each other, in order to assure that all necessary guarantees

are in place. This concerns in particular the assurance of data subject rights. The listing of responsibilities to be allocated under Art. 26 is, however, non-exhaustive and joint controllers are generally free to outline additional details of their relationship within such an agreement. They also need to make sure that the essence of the agreement is made available to the data subjects. These are, however, able to exercise their rights against any of the joint controllers, regardless of the content of the arrangement.

The Data Protection Authorities are in principle also not bound by any of the terms of such agreements and may exercise any of their powers equally against any of the parties determining the means and purposes of the processing jointly. They may, however, take the content of such into account when determining the amount of fines issued for a particular infringement. Data subjects can also claim compensation against any of the joint controllers under the same conditions which have already been outlined for single controllership. Since the GDPR does not, however, require any specific misconduct on the side of such an entity but simply the fact that an infringement of the Regulation occurred and that it caused damages, making any controller "involved" in the processing at any stage fully liable, a joint controller could potentially be required to compensate the individual for violations caused by their contractual counterpart. In that sense, the joint determination of means and purposes with other entities does bear quite significant risks. Where the (joint) controller has compensated the data subject for the entirety of the damages they will, however, be entitled to claim back part of that compensation from the other controllers or processors corresponding to the level of responsibility each of the parties bears with regards to the infringement and the damages caused by such, in accordance with Art. 82(5).

It can, therefore, be concluded that the legal figure of joint controllership constitutes a logical and crucial part of the data privacy landscape. From a purely theoretical perspective, the differentiation between instances where one controller uses another entity to act on behalf of them (processors), compared to where multiple entities determine means and purposes but independently from each other

(separate controllers), and those where two or more parties have a decisive impact on the processing operations and cooperate in order to achieve a common goal, is quite clear and seems to cover all possible scenarios. From a practical point of view there are, however, *often* difficulties in differentiating between those, especially considering that all of these terms are phrased quite broadly and flexibly for the purpose of technological neutrality. A multitude of definitions intending to cover a wide range of scenarios does, however, ultimately lead to overlaps which are frequently observed in that context. Based on the case law of the CJEU, current trends seem to point towards a strengthening of joint controllership instead of the traditional commissioned data processing.

D. Third Parties and Recipients

While the legal figures of controllers, processors, and joint controllers presented in the previous chapters constitute the main roles parties can take with regard to the processing of personal data, Article 4 No. 9 and 10 also introduce two additional functions which may be taken, namely those of third parties and recipients. These roles are, however, very different both in significance and effect to the previously described ones, as the Regulation does not provide for any responsibilities or obligations resulting from them.[692] In that sense, they are at times described as "relative concepts" based on the fact that they fulfil the function of describing a certain type of relation taken towards the controller or processor, rather than taking on an independent position in the processing of personal data.[693] While their impact and relevance in the context of data protection law is therefore not nearly as significant as that of the previously discussed actors, it is still important to consider them in order to have a full picture of all potential roles and responsibilities that might be taken with

---

[692] *EDPB*, Guidelines 07/2020, para 83; Kühling/Buchner / *Hartung*, Art. 4 Nr. 10 DSGVO, para 5.

[693] *EDPB*, Guidelines 07/2020, para 83; Kuner and others / *Tosoni*, Art. 4(10), 170, 171.

regards to a specific set of personal data or overall processing activity.

I. Third Party

Article 4 No. 10 defines a third party as *"a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data"*. The term is therefore defined in the negative, essentially stating who is not to be considered as a third party, namely the main actors outlined by the GDPR (controllers, processors, and data subjects), as well as any individual who is under the authority of those.[694] The purpose of this term thereby mainly lies in the differentiation from other parties, which are given explicit rights and responsibilities under the GDPR.[695] This will predominantly become relevant in the context of data transmissions to other parties.[696]

1. Definition

Similarly, to all of the other functions defined in the GDPR, there is no limitation as to the type of entity which can be considered a third party, again including all sorts of natural and legal persons. Typical examples of third parties include for example individuals who, based on the type of function they fulfil, process personal data on their own terms without being under the authority of the controller, such as for example independent consultants, freelancers, or contractors.[697] Likewise, where a company is part of a larger corporate group but still legally separate, they may be considered a third party if they are

---

[694]Kuner and others / *Tosoni*, Art. 4(10), 170, 172; Kühling/Buchner / *Hartung*, Art. 4 Nr. 10 DSGVO, para 8; Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 59.

[695]Kühling/Buchner / *Hartung*, Art. 4 Nr. 10 DSGVO, para 5; Specht/Mantz / *Mantz/Marosi*, '§ 3 Vorgaben der Datenschutz-Grundverordnung', para 24.

[696]Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 98; Specht/Mantz / *Mantz/Marosi*, '§ 3 Vorgaben der Datenschutz-Grundverordnung', para 24.

[697]Kühling/Buchner / *Hartung*, Art. 4 Nr. 10 DSGVO, para 6; *EDPB*, Guidelines 07/2020, para 87.

neither a controller nor a processor for a processing activity.[698] The same, however, does not apply for dependent branches or subsidiaries.[699]

Whereas the concepts of controller, processor, and data subject are clearly defined by the Regulation, making the distinction relatively clear, the same is not true for persons who *"under the direct authority of the controller or processor, are authorised to process personal data".* It is generally assumed that this refers to individuals who are part of the legal entity of the controller or processor.[700] This particular inclusion is of little practical relevance since actions of employees are presumed to be actions of the controller or processor themselves, and any processing performed by such outside of the given instructions would make the "rogue employee" a controller in their own right.[701] It is, however, imaginable that an individual would process data without their employer's authorisation without intending to use it for their own purposes, which would result in the excluding of the possibility of controllership and make them a third party.[702] In consideration of the used wording it is, however, not clear how legal representatives or guardians of the data subject are to be classified in that regard.[703] Considering them as third parties, especially if they are acting on behalf of the data subject, would make little sense and arguably act against their interest, since it might preclude some individuals, for example minors, from effectively exercising their rights. For this reason, such an interpretation should not be followed.[704]

---

[698]Kuner and others / *Tosoni*, Art. 4(10), 170, 172; *EDPB*, Guidelines 07/2020, para 87.

[699]Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 100.

[700]*EDPB*, Guidelines 07/2020, para 86.

[701]Kühling/Buchner / *Hartung*, Art. 4 Nr. 10 DSGVO, para 9.

[702]Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 60; *EDPB*, Guidelines 07/2020, para 86.

[703]Sydow/Marsch / *Ziebarth*, Art. 4, para 163.

[704]ibid.

2. Relevance

As already mentioned, third parties are mainly relevant for the purpose of differentiating such from the main actors concerned with the processing of personal data and are not given any rights or responsibilities under the GDPR. They, or rather their interests, can however become quite important when it comes to the determination of a legal basis for the processing of personal data. Article 6(1)(f) provides that such processing will be lawful where it is *"necessary for the purposes of the legitimate interests pursued by the controller or by a third party"*. While instances where a controller would decide to process personal data for another parties' interest are probably rare, this is still a relevant addition which is likely to be used for the transmission of personal data where another entity might have a strong interest in such.[705]

Also, while not explicitly mentioned, the interests of third parties can also be used as a legal basis for processing under Art. 6(1)(d) and 9(2)(c), both of which include the vital interests of "another natural person" additionally to those of the data subject into their scope. Such a natural person will, in most instances, presumably be a third party in the meaning of Art. 4 No. 10.[706] The inclusion for the protection of vital interests of third parties was likely deemed necessary by the lawmakers due to the fact that public authorities are precluded from using legitimate interest under Art. 6(1)(f) as a legal basis, thereby making it necessary to create a potential alternative for such, at least in crucial situations.[707]

II. Recipient

Last but not least, the General Data Protection Regulation introduces the role of recipient under Article 4 No. 9. Prior to its coming into force, there were in fact significant differences amongst Member States with regards to this particular term, with some not including it

---

[705]Kuner and others / *Kotschy*, Art. 6, 321, 337.
[706]ibid 334.
[707]ibid 334.

into their respective national data protection law at all and others introducing quite elaborate and detailed definitions.[708]

1. Definition

In accordance with Art. 4 No. 9, recipient means *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not"*. In contrast to the role of "third party", this definition is therefore not intended to differentiate between recipients and other actors but rather constitutes a superordinate concept including all types of entities, regardless of their legal qualification.[709] While there have been multiple attempts in the legislative process to at least partially limit this definition, the end result is quite broad, essentially including any person who receives personal data in any form.[710] If, therefore, a controller discloses personal data to third parties including other controllers, processors or even joint controllers, all of these will be considered as recipients in the meaning of Art. 4 No. 9.[711] Employees of the controller, dependent branches, and subsidiaries, as well as any other persons directly under the authority of the controller, will not fall under that definition.[712]

Also explicitly excluded from the definition of "recipient" in the second sentence of Art. 4 No. 9 are public authorities *"which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law"*. More specific examples of such

---

[708]Kuner and others / *Tosoni*, Art. 4(9), 163, 166.

[709]Kühling/Buchner / *Hartung*, Art. 4 Nr. 9 DSGVO, para 5; Taeger/Gabel / *Arning/Rothkegel*, Art. 4 DS-GVO, para 267.

[710]Kuner and others / *Tosoni*, Art. 4(9), 163, 166; Kühling/Buchner / *Hartung*, Art. 4 Nr. 9 DSGVO, para 3.

[711]*EDPB*, Guidelines 07/2020, para 90; Kuner and others / *Tosoni*, Art. 4(9), 163, 166; Kühling/Buchner / *Hartung*, Art. 4 Nr. 9 DSGVO, para 5; Taeger/Gabel / *Arning/Rothkegel*, Art. 4 DS-GVO, para 274.

[712]Kühling/Buchner / *Hartung*, Art. 4 Nr. 9 DSGVO, para 5; Taeger/Gabel / *Arning/Rothkegel*, Art. 4 DS-GVO, para 272.

are provided in Recital 31, which includes tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets, in that scope. It is, however, important to note that these types of entities are not automatically precluded from being considered as recipients but only in instances where they receive a specific set of personal data in the context of a particular inquiry in accordance with Union or Member State law.[713] The legal basis of their processing would, therefore, either need to be Art. 6(1)(c) or (e).[714] An example for such a Union law, falling under the scope of Art. 4 No. 9, can even be found directly in the GDPR, as Art. 58(1)(e) provides national supervisory authorities with the power to access all the personal data and other information necessary for the performance of their tasks.[715] Similarly, French tax authorities are, for example, allowed to request disclosure of specific information where this is necessary for the purpose of a tax fraud investigation.[716]

2. Relevance

Whereas the main relevance of the role of the third party could be found in the context of selecting a legal basis for the processing of personal data, the function of recipient is mentioned in multiple parts of the Regulation.

---

[713] Kuner and others / *Tosoni*, Art. 4(9), 163, 167; Kühling/Buchner / *Hartung*, Art. 4 Nr. 9 DSGVO, para 5.

[714] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 9 DSGVO, para 7.

[715] Kuner and others / *Tosoni*, Art. 4(9), 163, 167.

[716] ibid.

a) Data Subject Rights

The most central relevance of the term can arguably be established in the context of data subject rights.[717] First of all, the recipients or categories of recipients of personal data are amongst the information which has to be provided to the data subject by the controller in accordance with Art. 13(1)(e) and 14(1)(e). Article 14(3)(c) also clarifies in that context that any changes to recipients would need to be communicated to the affected individual, at the latest when the data is first disclosed. In the same vein, the recipients and categories of recipients, in particular those which are located in third countries, are also amongst the details to be included in an answer to a data subject access request, as provided in Art. 15(1)(c). Where a controller discloses personal data to any recipients and a data subject has put forward a request for rectification, erasure, or restriction of processing, Article 19 also provides that the controllers have the responsibility to communicate this fact accordingly to any such recipient, unless this should be impossible or involve a disproportionate effort.

b) Record of Processing Activities

Article 30(1)(d), introducing the requirement of maintaining a record of processing activities for controllers, also includes information about the categories of recipients to whom personal data is or will be disclosed amongst the facts which should be documented. Especially recipients in third countries or international organisations should be accounted for therein. Considering the fact that this information needs to be disclosed to the data subjects in the privacy notice and at any given time on demand, covering it within the ROPA seems quite logical and likely advantageous for the controller, especially since it can also be used to contact these parties where required by Art. 19. It also allows a full overview of the company's data

---

[717] Kühling/Buchner / *Hartung*, Art. 4 Nr. 9 DSGVO, para 4; Kuner and others / *Tosoni*, Art. 4(9), 163, 165; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 9 DSGVO, para 1.

flow and is therefore likely to be accessed by the supervisory authorities as well.

c) International Data Transfers

The first mention of recipients in the context of international data transfers can be found in Article 46, which outlines the various forms in which controllers as well as processors, can assure and also demonstrate the assurance of appropriate safeguards for transfers of personal data to third countries and international organisations. Amongst those, Paragraph 3 therein lists the option of demonstrating such through contractual clauses authorised by the competent supervisory authority, which may be concluded between controllers or processor and the controllers, processor or *the recipient* of personal data. Here, the use of the term "recipient" seems to fulfil the purpose of widening the scope of these clauses and clarifying that data transfers to parties other than another controller or processor are also possible but should be subject to the same safeguards.

The second instance in which the Regulation mentions recipients in that regard can be found in Art. 49, which provides derogations for the general rules for specific situations. Paragraph 2 therein clarifies that in the context of transfers made from a register, which is intended to provide information to the public in accordance with Union or Member State law and which is open to consultation by the public or individuals demonstrating a legitimate interest, such transfers should not include the entirety of the data contained in the register. The second sentence then further stipulates that where such registers are intended for consultation by individuals who bring forward a legitimate interest in the data, the transfer should only be made on request of those people or *"if they are to be recipients"*. This addition is in fact quite crucial since it opens the possibility for the interested parties to be represented by someone else or have other actors act on their behalf, without having to exercise their right themselves.

d) Supervisory Authorities

Last but not least, recipients are also mentioned in the context of the powers of supervisory authorities. First, they are considered twice in the context of the corrective powers of the DPA, namely in Art. 58(2)(g) and (j), which allow them to order (1) the notification of recipients regarding the data subject requests put forward under Art. 16, 17 or 18; and (2) the suspension of data flows to third countries or international organisations, respectively. In that sense, these powers directly correlate to the relevance of recipients in the context of aa) Data Subject Rights and cc) International Data Transfers outlined previously. Finally, they are also referred to in the context of the imposition of administrative fines. Article 83(5)(c) provides that in cases where infringements of the rules concern the transfers of personal data to a recipient in a third country or an international organisation, fines up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, may be issued.

III. Interim Conclusions: Third Parties and Recipients

Additionally, to the central roles of controllers and processors involved in the processing of personal data, the GDPR also introduces the terms “third parties” and “recipients”. These actors, however, do not take an independent position in the processing activity but rather fulfil the function of describing a certain type of relation taken towards the controller or processor.

Third parties are defined in the negative as any natural or legal person, other than any of the principal actors involved in the processing of personal data (controllers, processors and data subjects) or individuals under their authority fall under that term. The relevance of the term, therefore, mainly lies in the purpose of differentiating third parties from stakeholders bearing rights and responsibilities under data protection law. The only instance in which third parties might in fact impact the processing of personal data involves the consideration of their interests in determining a legal basis for the processing operation in accordance with Art. 6(1)(d) and (f), and Art. 9(2)(c).

Recipients are, per definition, any party to which personal data is being disclosed. This means all types of entities can be a recipient, regardless of their legal qualification, including controllers, processors, and third parties, therefore making this term a superordinate concept. The terms become relevant in multiple contexts within the GDPR. The main impact arguably materialises in the context of data subject rights, as the involvement of any recipients needs to be communicated to the data subject accordingly. Likewise, recipients need to be informed of any incoming data subject request concerning data which has been disclosed to them. Recipients, however, also have some bearing in the context of the record of processing activities and international data transfers, as well as the powers of the supervisory authorities.

Chapter 4

Designation of Roles for Personal Information Managament Systems

The first section of Part 2 defined all the different roles which may be assigned to the party involved in the processing of personal data in accordance with the General Data Protection Regulation, as well as the criteria used for their determination. It is also evidenced that such a designation of an entity as either a controller, processor, joint controller, separate controller, third party, or recipient, is accompanied by a number of significant legal implications, not only for the parties involved in the processing but most importantly for the data subject. How, where, and to what extent individuals will be able to exercise their rights, expect guarantees, or even demand compensation will all depend on the legal designation of the actors involved. While the Regulation has introduced clear criteria for the designation of these respective roles, factors such as increasingly complicated corporate structures, general trends of interconnectedness, and global data sharing, as well as the introduction of new technologies can make an accurate distinction quite challenging. This is also evidenced by the recent case law of the CJEU, which while attempting to add some clarity in this regard, has also raised a number of new questions.

The purpose of this thesis, however, does not lie in debating the legal designation of roles under the GDPR in general but specifically in the context of a new privacy friendly emerging technology: Personal Information Management Systems. Part 1 provided an introduction to these tools, which can broadly be described as *“technologies and ecosystems, which aim to empower individuals to control*

the collection and sharing of their personal data".[1] The need for such has been identified based on observation that there is an inherent asymmetry of power between data subjects and the businesses processing their personal data, effectively hindering individuals from fully controlling their information and properly exercising their rights. PIMS intend to bridge that gap by providing a multitude of functionalities that would allow a better overview, understanding, communication and, most importantly, control over one's dataflows. Since the term is, however, inherently broad and the specifics of these technologies are still largely in development, there is a wide array of tools that fall under this term, introducing a multitude of functionalities.

As is so often the case with newly emerging technologies there are, however, a number of questions and legal implications that still do not seem to be entirely defined in the context of their development. Personal Information Management Systems are no exception in that regard. While it is clear that they intend to support and empower data subjects in managing their relation with the controller, there seems to be little consideration as to the roles they are taking with regards to the processing activity. Publications on the subject rarely take a deeper or more fine-grained look into that question.[2] Where the subject of their legal designation under the GDPR does come up, they usually simply refer to the need of determining such on a case-by-case basis, depending on the specific functionalities of

---

[1] *EDPS*, Opinion 9/2016, para 4. Also similarly: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht, 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[2] The question of controllership is for example not at all considered in: *Attoresi/Moraes*, TechDispatch #3/2020; *European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016) 10.

the PIMS.[3] While all acknowledge the importance of accurately designating those roles based on the functionalities, additional clarifications or practical examples are rarely included.[4] Where an exhaustive analysis is in fact performed, it usually only concerns one specific type of service offering, thereby potentially overlooking implications relevant to tools offering multiple functionalities at once.[5]

In that sense, a comprehensive overview of the different scenarios and the possible designation of roles for these systems, as well as the consequences arising as a result, seems more than warranted. This is especially the case considering the whole purpose of PIMS, which is creating a more transparent environment for data subjects under which they can easily navigate the processing of their personal data. In that sense, the standard for transparency should be even higher for these types of service offering than for any other type of operation, making the creation of clear rules even more necessary. Part 1 of this thesis established some general categories of tools based on the system's objectives, as well as the technical set-up, and including an overview of how their functionalities attempt to strengthen the data subject rights. Part 2 Chapter 3 presented the legal roles parties can take with regards to a processing activity in accordance with the GDPR. The following section will, therefore, try to subsume the presented service offerings, whether currently or still under development, and analyse I these PIMS should therefore take vis-a-vis the data subject.

---

[3] *EDPS*, Opinion 9/2016, para 45ff; *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 9; *Riechert*, in: Neue Wege, 38, 45f; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

[4] *EDPS*, Opinion 9/2016, para 45ff; *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 9; *Riechert*, in: Neue Wege, 38, 45f.

[5] A comprehensive overview and discussion of the issue can for example be found in: *Santos and others*, in: Privacy Technologies and Policy, 47, 47ff. The scope of the analysis is however limited to consent management platforms using the Transparency and Consent Framework proposed by IAB Europe, with a specific focus on Quantcast and OneTrust.

A. Storage

As has been outlined under Part 1 Chapter 2: A. Storage in the context of Personal Information Management Systems, data can either be stored locally or within the cloud.

I. Local Storage

Local storage means that all data is physically kept within the user's device. As with most applications, this will usually be a smart phone or computer. Some providers such as the "Freedom Box" even offer a completely separate hardware.[6] While the PIMS facilitates and allows the installation of its application on the user's device and controls the functionalities and setting of such, this provides more of a generalised framework for the data processing operation. The PIMS has no control or access over the data, neither does it have any explicit knowledge of what type of information is being stored, for what purposes, and for how long the user will be storing it. It is, therefore, generally accepted that decentralised data storage does not lead to the consideration of a PIMS as a controller or processor under the GDPR, making the provider a third party.[7] Quite similar considerations regarding the responsibilities for decentralised storage have in fact been discussed at length in the context of controllership over Bitcoin and while a consensus has still not been reached, it is generally accepted that the developer cannot be considered a controller under Art. 4 No. 7 of the GDPR.[8]

It is, however, important to note that this outcome, excluding the role of a provider of decentralised storage as a controller or processor, pertains only to this isolated functionality. As has been outlined

---

[6]See for example: Freedom Box, https://freedombox.org/about/ (accessed: 24 October 2025).

[7]*Riechert*, in: Neue Wege, 38, 45.

[8]*Erbguth/Fasching*, 12 ZD 2017, 560, 564; *Bechtolf/Vogt*, 2 ZD 2018, 66, 69; *Schrey/Thalhofer*, 20 NJW 2017, 1431, 1433f; *Finck*, 4 EDPL 2018, 17, 26.

in Part 1 and will be analysed further, a PIMS will usually offer a number of additional features, resulting in more involvement in the processing operation and thereby potentially in a shift of those roles. For this reason, it cannot be assured that a PIMS using decentralised forms of storage would automatically be considered a third party. Developers of the IoT Databox model, for example, seem to consider their application as a processor.[9] Dataswift, on the other hand, qualifies itself as either a controller or a processor, depending on the type of operation.[10] The separate consideration of these elements is, however, still important in light of the fragmented approach to data processing introduced by the CJEU in the case of *Fashion ID*.[11] In that sense, it can be concluded that a provider of a Personal Information Management System cannot be considered a controller or processor for the local storage of data on the user's device.

II. Cloud Storage

Cloud service providers have traditionally been considered as processors under the Data Protection Directive and this position is still the prevailing opinion to this day.[12] This is despite the fact that cloud providers *often* have a considerable impact on the processing of personal data through defining elements such as the applied hardware and software, how data should be stored and where, what type of

---

[9] *Crabtree and others*, 4 J Reliable Intell Environ 2018, 39, 43.

[10] See: Data Swift, 'Personal Data Account (PDS) Owner Agreement', Section 7 "Data Protection", https://cdn.dataswift.io/legal/hat-owner-terms-of-service.pdf, (accessed: 24 October 2025).

[11] *Zalnieriute/Churches*, 83 MLR 2020, 861, 861; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Becker and others*, 12 IDPL 2022, 207, 212; *Paun*, 9 EuCML 2020, 35, 36f.

[12] *EDPB*, Guidelines 07/2020, para 82; *Funke/Wittmann*, 5 ZD 2013, 221, 221; *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356, 366; *Lynn*, in: Data Privacy and Trust, 21, 30; *Jotzo*, Der Schutz, para 133.

security measures are to be deployed, who and under which circumstances might access the data, or even when it should be deleted.[13] Still these decisions are predominantly defined as "non-essential" means and it is assumed that the main purpose of the processing lies with another entity, i.e., the controller, as a cloud provider would usually only have a commercial interest in performing their contractual obligation.[14] Some also point out that this assumption is in the interest of the cloud provider itself, who as a processor will be assigned a lower degree of responsibility under the GDPR, thereby solidifying this pre-conceived notion in practice.[15] While contracts with cloud providers are, however, still predominantly set-up as commissioned data processing under Art. 28, in practice there is a broad debate on the issue[16] which is why it is necessary to take a closer look at the subject, considering the various types of cloud services available on the market, as well as the specifics relevant to their deployment in Personal Information Management Systems.

1. Types of Clouds

The previous analysis of possible data storage options broadly divided the types of cloud storage into public, private, and hybrid clouds.[17] The type of cloud storage solution will significantly affect the way in which decisions regarding the processing of personal data are being conducted and by whom, which is why it needs to be considered in the determination of the roles and responsibilities of the parties.

---

[13] *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356, 366; *Funke/Wittmann*, 5 ZD 2013, 221, 222f.

[14] *Funke/Wittmann*, 5 ZD 2013, 221, 222f; *Jotzo,* Der Schutz*,* para 133; *Sury*, 44 Informatik Spektrum 2021, 376, 376; *Petri*, 7 ZD 2015, 305, 306.

[15] *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356, 366.

[16] *Hon/Millard/Walden*, 2 IDPL 2012, 3, 7-14; *Jotzo,* Der Schutz, para 132; *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356, 366.

[17] See Part 1 Chapter 2: A. I. 2. Cloud Storage.

a) Public Cloud

Public clouds are usually provided by large vendors which take over the deployment and maintenance of the servers.[18] A review of the currently offered contracts by the largest and most popular public cloud providers Amazon Web Services, IBM, Google Cloud, and Microsoft Azure evidences that all of these consider themselves as processors for the cloud storage services provided by them.[19] At the same time, however, these data processing agreements set out the specifics terms of the processing in advance, including such elements as the purpose, subject matter, and duration of the processing, as well as data subjects and specific technical and organisational measures. While these "details" are generally kept incredibly vague,[20] it clearly evidences that these model agreements are intended to be executed in this exact form. This means that there is

---

[18] *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 38f.

[19] AWS Data Processing Addendum, https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf (accessed: 20 October 2025); IBM Data Processing Addendum, https://www.ibm.com/support/customer/csol/terms/?id=Z126-7870&lc=en#detail-document (accessed: 20 October 2025); Google Cloud Data Processing Addendum, https://cloud.google.com/terms/data-processing-addendum (accessed: 20 October 2025); Microsoft Products and Services Data Protection Addendum, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021 (accessed: 20 October 2025).

[20] See for example: AWS Data Processing Addendum Section 1.3 Details of Processing – 1.3.3 Purpose "*The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time*"; 1.3.6 Categories of Data Subjects "*The data subjects could include Customer's customers, employees, suppliers and End Users*", https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf (accessed: 20 October 2025); Google Cloud Data Processing Addendum, Appendix 1: Subject Matter and Details of the Data Processing, "*Google will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with this Addendum*", "*Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or by its End Users*", https://cloud.google.com/terms/data-processing-addendum (accessed: 20 October 2025).

essentially no room for customisation, changes, or actual "instructions" to be provided by the customers which would, as per definition, be required for the consideration as a processor under the GDPR. This, in fact, is a commonly known issue with many sources pointing out this exact problem in the context of deploying large vendors for the establishment of cloud storage solutions.[21]

The considered alternatives are, however, arguably equally unsatisfying. While the applicability of joint controllership might be considered[22] taking into account the extent of the decisions made by the cloud provider, the lack of actual interest in the underlying data, apart from the provision of the ordered service, will usually preclude them from determining the purposes of processing, thereby falling outside of the definition of controller.[23] If, however, the very broad definition of "joint purposes" applied by the CJEU in the case of *Fashion ID* would be used where the presence of "economic interests" on the side of both parties were considered sufficient,[24] this might after all not present a hindrance in assuming a joint controllership for public cloud deployment. The second alternative put forward by some sources is the consideration of a cloud provider as neither controller, nor processor, unless the service includes automated data replication for business continuity.[25] Based on this notion, the cloud providers could be qualified as neutral intermediaries, the liability of which could be applied analogously to the intermediary liability provision under the Electronic Commerce Directive.[26] This would, however, essentially exclude any type of liability of such providers under the

---

[21] *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356 *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356[21] *Blume*, IDPL 2013, 140, 142; *Janssen/Cobbe/Norval/Singh*, 10 IDPL 2020, 356, 366; *Jotzo,* Der Schutz, para 132; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 87.

[22] *Völker/Schnatz/Breyer*, 6 MMR 2022, 427, 432.

[23] *Funke/Wittmann*, 5 ZD 2013, 221, 222f; *Jotzo,* Der Schutz, para 133; *Sury*, 44 Informatik Spektrum 2021, 376, 376; *Petri*, 7 ZD 2015, 305, 306.

[24] Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 80.

[25] *Hon/Millard/Walden*, 2 IDPL 2012, 3, 11.

[26] *Hon/Millard/Walden*, 2 IDPL 2012, 3, 14.

GDPR and can therefore not be considered as in the interest of effective and completed protection of the data subject required by the CJEU.

In that sense, the qualification as a processor, while not ideal, is still probably the most appropriate. The strong influence of such a processor should not automatically hinder such as assumption, since after all there is no rule governing that the controller needs to be the stronger or more experienced counterpart. The amount of authority held by the cloud provider is based on two components. First of all, as is the case with many IT-Services, the provider of a public cloud solution will often have a significantly higher degree of technical knowledge than the client, which is why they are so involved in the determination of the technical and organisational measures.[27] Secondly, the imbalance of powers observed between the parties does not result from the processing operation itself, but rather the inherent imbalance between actors which are stronger or weaker economically.[28] The fact that global corporations have a stronger negotiating position than small- or medium-sized businesses, will hold true regardless of the type of contract and the standardised form in which the presented providers conclude is applied for all of their customer agreements, not just the DPAs.[29] The EDPB also explicitly recognises in that context that processors are not precluded from offering preliminary defined services and that the essential determination

---

[27] *EDPB*, Guidelines 07/2020, para 78; *Hon/Millard/Walden*, 2 IDPL 2012, 3, 7; *Völker/Schnatz/Breyer*, 6 MMR 2022, 427, 431.

[28] *Blume*, IDPL 2013, 140, 142.

[29] See for example the standardized: AWS Service Level Agreements, https://aws.amazon.com/legal/service-level-agreements/?aws-sla-cards.sort-by=item.additionalFields.serviceNameLower&aws-sla-cards.sort-order=asc&awsf.tech-category-filter=*all (accessed: 20 October 2025); IBM Cloud Service Level Agreements ,https://cloud.ibm.com/docs/overview?topic=overview-slas (accessed: 20 October 2025); Google Cloud Platform Service Level Agreements, https://cloud.google.com/terms/sla (accessed: 20 October 2025); Microsoft Azure Service Level Agreements, https://azure.microsoft.com/en-us/support/legal/sla/ (accessed: 20 October 2025).

made by the controller lies in selecting this specific service offering.[30] This also makes sense, since even in scenarios where customers are left with a "take it or leave it approach", the possibility of deciding for or against a specific provider still exists and allows for full authority over the processing.[31] After all, while data storage on a public cloud might be the most economically advantageous, there are many alternatives which can and should be considered.

b) Private Cloud

The presented problems in establishing the legal qualification of public cloud providers will bear limited significance in the context of Personal Information Management Systems; providers of such, offering storage as part of their business model, largely rely on private, rather than public cloud storage.[32] A prominent exception, however, is Dataswift, which is designed to be hosted on Amazon Web Services (AWS) cloud servers.[33] Due to the connected security risks, as well as taking into account customer preferences, this model, however, does not seem like a particularly viable or popular solution in the deployment of PIMS.[34] In the case of private cloud solutions, the identification of a data controller is in fact significantly simplified, since the processing operations are far more centralised and all decisions regarding the technical deployment, the data location,

---

[30] *EDPB*, Guidelines 07/2020, para 82.

[31] *Jotzo,* Der Schutz, para 132; *Völker/Schnatz/Breyer*, 6 MMR 2022, 427, 431.

[32] See for example: Data Vaults, https://www.datavaults.eu/ (accessed: 20 October 2025); Cozy Could, https://cozy.io/en/ (accessed: 20 October 2025); Nextcloud, https://nextcloud.com/ (accessed: 20 October 2025); ownCloud, https://owncloud.com/ (accessed: 20 October 2025); Meeco Vault, https://www.meeco.me/ (accessed: 20 October 2025).

[33] Dataswyft, https://www.dataswift.io/news/privacy-property-wealth-creation-in-a-decentralized-data-economy (accessed: 20 October 2025).

[34] For more details refer to Part 1 Chapter 2: A. I. 2. a) Public Cloud.

maintenance, and security measures are made by the customer.[35] As a result, the cloud customer who will determine the means, as well as the purposes of processing personal data, will naturally take the role of a data controller.[36] Providers tasked only with the maintenance of the infrastructure will, on the other hand, be considered processors if they are monitoring the processing activity as well, or alternatively solely as third party IT-service providers.[37]

c) Hybrid Cloud

The establishment of general rules regarding the roles and responsibilities for hybrid cloud models is quite challenging. Since the term applies to all types of models combining elements of public and private clouds, no uniform form of deployment can be identified. Considering the above analysed scenarios in which the cloud provider would either be considered a controller or processor; it can at least be assumed that the same would apply in the case of hybrid cloud storage models. This specification is quite insignificant but it does narrow down the possibilities slightly. As always, in order to identify the specific role, the cloud provider would take with regards to the processing of personal data, the particular circumstances of each case would therefore have to be taken into account.

It should, however, be noted that hybrid cloud solutions will typically require a higher degree of customisation, than the other two, more standardised models. Since the services from both domains need to be integrated into each other, the specific needs of the customer need to be communicated, specifically with regards to the classification and division of certain datasets and the security requirements applicable to such.[38] This means that the relationship between

---

[35] *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 38; *DSK*, Cloud Computing, 7; *Mell/Grance*, The NIST, 3; *Schröder/Haag*, 4 ZD 2011, 147, 148.

[36] *DSK*, Cloud Computing, 7; *Völker/Schnatz/Breyer*, 6 MMR 2022, 427, 432; *Schröder/Haag*, 4 ZD 2011, 147, 148.

[37] *Hon/Millard/Walden*, 2 IDPL 2012, 3, 11.

[38] *Yang/Xiong/Ren*, 8 IEEE Access 2020, 131723, 131724; *Völker/Schnatz/Breyer*, 6 MMR 2022, 427, 428f.

the customer and the provider will likely be more extensive than in the case of more standardised solutions, as it requires a higher degree of communication.[39] Where such communication takes place and the parties make joint decisions regarding the means of processing, the applicability of joint controllership could potentially be considered. Joint decision making should, however, be distinguished from simple advice or recommendations issues by the cloud provider. If the decisions are still being made solely by the customer and the processing takes place for the customer's benefit, the cloud service provider is still to be considered a processor.[40]

d) Interim Conclusions: Cloud Storage

For all the considered cloud types, the customer will typically be qualified as a data controller under the GDPR. Cloud providers on the other hand may be considered as processors, joint controllers, or even third parties, depending on the specific circumstances and the extent of the provided service. Providers of public clouds will typically constitute processors as they usually have no interest in either the type or purposes for storing the customer's data but will, to a large extent, determine the means of the processing by pre-defining the available technical parameters. A similar qualification will likely apply to any service providers responsible for maintaining the infrastructure in the context of running a private cloud. They may, however, also fall under the definition of a third party especially where no data is being accessed. Hybrid cloud services will, on the other hand, require a higher degree of customisation, potentially opening the possibility for joint controllership where both means and purposes are determined jointly.

---

[39] *Völker/Schnatz/Breyer*, 6 MMR 2022, 427, 428f; *Hon/Hörnle/Millard,* 26 Int. Rev. Law Comput. Technol. 2012, 129, 130; *Rajan/Shanmugapriyaa*, 1 IOSRJCE 2012, 38, 39.

[40] *Funke/Wittmann*, 5 ZD 2013, 221, 222f; *Jotzo,* Der Schutz, para 133; *Sury*, 44 Informatik Spektrum 2021, 376, 376; *Petri*, 7 ZD 2015, 305, 306.

2. Type of Customer

The above conclusions are, however, missing a crucial element requiring consideration, namely the type of customer deploying a cloud service provider. The general assumption, which in legal practice, DPA guidelines, and literature qualifying the customer as the data controller, is largely based on considerations of business practice by which the client will be a natural or legal person wishing to store personal data, concerning other individuals, for their own purposes.[41] In most instances, this will be a company or public authority needing to outsource the storage of their data, either personal or not. The personal information contained in such datasets will thereby typically concern their customers, employees, or individuals with which business communication or other type of contact is maintained. In such scenarios, it naturally makes sense that the customer should in either case retain controllership over the data since they are likely the ones collecting the information, communicating with the data subjects, and determining the purposes for which it is being used.

This, however, is not the case with Personal Information Management Systems. Here, the "customer" will be the data subject wishing to store their own personal data for security reasons. While some have pointed out that where an individual user, storing their own personal data in the cloud, is seen as the customer and the cloud provider would likely be considered a controller, this is not necessarily the position supported by the most popular cloud storage solutions themselves.[42] It could be argued that the personal information of one person may inadvertently also "relate to" other individuals, making it their personal data as well,[43] creating the need for responsibility for

---

[41] *Schumacher*, in: IT-Outsourcing, 432, 436; *Funke/Wittmann*, 5 ZD 2013, 221, 221; *Schröder/Haag*, 4 ZD 2011, 147, 147f; *Jotzo,* Der Schutz, para 133.

[42] *Hon/Millard/Walden*, 2 IDPL 2012, 3, 7.

[43] Pictures may include other individuals than just oneself, communication data will usually also include the replies of the other side, bank accounts, real estate, cars or other property may be shared, even health or genetic data can be used to deduce information about family members (for example where it concerns genetic characteristics or diseases).

the handling of their data. Such an assumption is, however, inconsistent with the entire purpose of PIMS which per definition lies in *"empowering individuals to control the collection and sharing of their personal data".*[44] In that sense, if controllership of the customer was assumed, the data subject would be a controller of their own personal data. The PIMS would then either act as a processor or potentially joint controller.

Whether a data subject could be considered a controller for their own personal data has already been discussed under Part 2 Chapter 3: A. II. 2. b) Data Subject. As has been established, the issue is subject to a heated academic debate, especially in consideration of the narrow interpretation of the household exemption, combined with the gradual broadening of the term "controller" by the CJEU.[45] It has, however, been concluded that such an outcome would not be in line with the primary purpose of the Regulation, which is the protection of natural persons where their data is being processed.[46] Individuals would face significant difficulties in exercising their rights, awarded in Chapter III of the GDPR. [47] Such a reading would also go against the aim of assuring *"effective and complete"* protection established by the CJEU's case law.[48] Based on that, it is the view presented in this thesis that such a possibility should be categorically rejected.

The incompatibility of the assumption under which the data subject would be considered a controller for the processing of their own

---

[44]*EDPS*, Opinion 9/2016, para 4.

[45]*Wagner*, 7 ZD 2018, 307, 307; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Finck*, Blockchain Regulation, 101; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212; *Finck*, 11 IDPL 2021, 333, 338.

[46]Sydow/Marsch / *Raschauer*, Art. 4, para 119; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212.

[47]*Edwards and others*, IPR 2019.

[48]Sydow/Marsch / *Raschauer*, Art. 4, para 119; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212.

personal data with the purpose of the processing, is even more evident in the case of Personal Information Management Systems. If controllership of the individual user would be accepted, all responsibility for the processing would also lie on their side, leaving them without any protections under the GDPR. In effect, the use of a PIMS storage system would be one of the most insecure forms of storing personal data, which most certainly is not what supporters of these solutions intend to achieve. It is, therefore, without question that a provider of a secure storage solution should be considered the controller for the provided service, including both user-related personal data collected by them (for example metadata, log-in details etc.), as well as any type of information stored within their infrastructure. This position also seems to be supported by the European Data Protection Supervisor, who in their 2016 Opinion on PIMS, while remaining vague as to the division of roles and responsibilities for other functionalities, quite clearly stated that *"[w]ith respect to certain aspects of data processing, such as storage of data, there is usually no doubt that the PIMS will act as a controller, and therefore it is responsible for keeping the data secure"*.[49]

3. Current Practice

While it is the position presented here that PIMS providers should be considered a controller with regard to storage of personal data on their cloud servers, this does not necessarily represent the opinion of the providers themselves, which is why the designation of roles and responsibilities introduced by currently available service offerings should also be examined.

a) DataSwift

Dataswift allows users to create Personal Data Accounts (PDA) through which they can licence the data to apps and websites with a

---

[49] *EDPS*, Opinion 9/2016, para 44.

data wallet.[50] The platform is hosted on cloud servers of Amazon Web Services (AWS) self-reportedly in a form that *"adheres to local storage requirements of GDPR"*.[51] With regards to the question of controllership and liability, the Dataswift Personal Data Account (PDA) Owner Agreement specifies that Dataswift is the controller for personal data collected for the purposes of: establishment, operation and administration of the PDA; providing the services, including the management of Data Plugs and Data Debits; and the supervisions of compliance with the Acceptable Use Policy.[52] In the context of hosting or back-up of the HAT Data and File Storage, they are however qualified as a processor, acting on behalf of the customer.[53] For the data hosted in the PDA, Section 2.1(b) clearly establishes that the user, meaning the data subject, is to be considered the controller for all connected processing activities as they are the ones who decide *"how and why any Personal Data (…) will be used"*.[54]

b) Meeco

A similar approach seems to be taken by Meeco. The provider offers a "Secure Value Exchange" platform which includes (1) Secure Data Storage; (2) Verifiable Credentials; and (3) Digital Assets.[55] It also allows for the vault to be embedded into existing applications through authentication with an OpenID Connect provider.[56] In accordance

---

[50]Dataswift, https://www.dataswift.io/for-individuals (accessed: 20 October 2025).

[51]Dataswift, https://www.dataswift.io/news/privacy-property-wealth-creation-in-a-decentralized-data-economy (accessed: 20 October 2025).

[52]See: Data Swift Personal Data Account (PDS) Owner Agreement, Section 7.1, https://cdn.dataswift.io/legal/hat-owner-terms-of-service.pdf (accessed: 20 October 2025).

[53]ibid.

[54]ibid.

[55]Meeco, https://www.meeco.me/#home-main-content (accessed: 20 October 2025).

[56]ibid.

with Meeco's Privacy Promise & Policy, the company considers themselves the "controller" for any information collected as a result of visiting their website (browser type, language preference, time and date etc.); entered in a webform (name, e-mail address, country, preferred language etc.); or required to log into the service (e-mail address, name, password).[57] For the actual service offering they are, however, only qualified as a processor, based on the reasoning that "Meeco enables You to collect and direct us to process the data on Your behalf", again implying controllership on the side of the end user.[58] The set-up of an account is, however, quite complicated and involves multiple steps, requiring a certain amount of technical expertise[59] which might suggest that the service provider is aiming at legal entities setting up accounts for their clients as customers, rather than direct use by the data subject.

c) DataVaults

A different position has been taken by the Horizon 2020 funded project, Data Vaults.[60] The venture aims to provide individuals with a framework for leveraging personal data from various sources by constructing a unified personal data hub where all information is being securely retained and through which it can subsequently be shared with third parties in return for compensation.[61] The documentation on deliverable D.2.1 "Security, Privacy and GDPR Compliance for Personal Data Management" identifies four types of actors: (1) individuals, as data subjects; (2) the "Personal DataVaults" component, as part of the data subject; (3) the "DataVaults Cloud Platform", acting as a broker between individuals and organisations; and (4) data

---

[57]Meeco´s Privacy Promise & Policy, https://media.meeco.me/public-assets/legal/meeco-privacy.pdf (accessed: 20 October 2025), 6.

[58]Meeco´s Privacy Promise & Policy, https://media.meeco.me/public-assets/legal/meeco-privacy.pdf (accessed: 20 October 2025), 6.

[59]Meeco, https://docs.meeco.me/getting-started/setting-up (accessed: 20 October 2025).

[60]DataVaults, https://www.datavaults.eu/ (accessed: 20 October 2025).

[61]DataVaults, https://www.datavaults.eu/about/ (accessed: 20 October 2025).

seekers, asking for the individual's personal data.[62] Here the DataVaults' platform is considered the controller as it is intended to be used by an entity responsible for managing personal data.[63] Where an entity using the platform obtains the service of another company in order to manage part of the data or the processing activity, this vendor is qualified as a processor.[64] Data seekers are defined as recipients or processors, depending on whether or not they are going to further process the transferred information.[65] The data subject and their "Personal DataVault" on the other hand, while described as taking ownership of their data and managing it, are not assigned any additional roles under the GDPR.[66]

d) MyDex

MyDex offers a number of different components including a Personal Data Store, Personal Data Exchange Services, Identity as a Service, an included Platform, and a Web App Generator.[67] The Personal Data Store (PDS) is hosted in the cloud and is intended to enable individuals to collect, receive, and store their personal data.[68] While the MyDex Charter clearly establishes that they consider themselves as a provider of personal information management services and as *"owner and controller of the data architecture of MyDex Master PDS Data Schema"*,[69] it is not entirely clear whether this refers to

---

[62] https://www.datavaults.eu/wp-content/uploads/2020/11/DataVaults-D2.1-Security-Privacy-and-GDPR-Compliance-for-Personal-Data-Management.pdf (accessed 21 November 2024), 13.

[63] ibid 13.

[64] ibid 13.

[65] ibid 13.

[66] ibid 13.

[67] MyDex, https://mydex.org/platform-services/ (accessed: 20 October 2025).

[68] MyDex, https://mydex.org/platform-services/#personal-data-store (accessed: 20 October 2025).

[69] MyDex, https://dev.mydex.org/mydex-charter.html (accessed: 20 October 2025).

control in the sense of Art. 4 No. 7 of the GDPR. In the context of defining the roles and responsibilities of the involved actors they do, however, set out specific obligations *"pertaining to all participants except individuals using the platform"*.[70] In that sense, it seems to be clear that data subjects are not intended to take the roles of a data controller or to be burdened with any legal responsibility but rather that this should be divided amongst the platform itself and the entities potentially gaining access through it to the personal data.

III. Interim Conclusions: Storage

Local storage, by which all data is physically kept within the user's device, does not generally lead to the consideration of the service provider of such as either a controller or processor under the GDPR, since they are essentially only supplying the data subjects with a tool to process their own personal data but are not directly involved in the determination of the means or purposes of the processing. The determination of the respective roles and responsibilities of the parties is, however, significantly more difficult where customers' personal data is kept in cloud storage. Providers of cloud storage solutions are traditionally considered processors even though they *often* have considerable impact on the processing of personal data. Depending on whether or not a public, private, or hybrid cloud solution is being deployed, the distribution of roles might vary, potentially leading to their qualification as joint controllers or even third parties. This general lack of clear division between the different functions taken by the parties can also be observed within the examples of current offerings of Personal Information Management Systems, some of which accept controllership over the personal data stored on their systems, whereas others present themselves as processors or even third-party intermediaries, considering the end user the controller.

The consideration of a cloud customer as the data controller is commonly accepted and correct in traditional settings where cloud

---

[70] MyDex, https://dev.mydex.org/mydex-charter.html (accessed: 20 October 2025).

providers are deployed for the outsourcing of storage by entities processing the data of other individuals such as, for example, their clients or employees. In the case of Personal Information Management Systems, it would, however, lead to the outcome under which the data subjects would essentially be qualified as the controller for their processing of their own personal data, resulting in the fact that all legal responsibilities and liabilities would also be shifted onto them. This cannot be considered as acceptable in light of both the clear division between the different actors introduced by the GDPR and the purpose of the Regulation, which aims to protect natural persons from the illegal processing of their personal data. This interpretation would also clearly go against the aim of assuring *"effective and complete"* protection continuously established by the CJEU's case law. It should, therefore, be concluded that a provider of a secure storage solution is to be considered the controller for the provided service, including both user-related personal data collected by them and any type of information stored within their infrastructure.

B. Information

The second functionality of Personal Information Management Systems, analysed in this thesis, relates to the provision of information as required by Articles 13 and 14 of the General Data Protection Regulation. As has been presented previously under Part 1 Chapter 2: B. II. Obstacles, both controllers and data subjects experience significant hurdles in respectively providing and receiving transparent information with regards to the processing of personal data. A number of different types of PIMS attempting to alleviate these issues have already been developed and the functionality will most likely become even more relevant in the future. While solutions vary on both their design and set-up, for the purpose of this thesis these have been broadly divided into interpretative, auditing and responsive tools. Their respective legal functions as seen under the GDPR should therefore also be analysed based on this division.

I. Interpretative Tools

Interpretative tools serve the purpose of extracting the information relevant to each user from privacy policies and presenting it in a coherent and intelligible way, thereby in a sense providing an interpretation of the available text by translating it into a more comprehensible format. Since providing manual transcriptions is virtually impossible, these tools usually rely on a combination of natural language processing and either supervised or unsupervised machine learning.[71] Users will, for example, provide the URL of the privacy policy they wish to have analysed or enter the entire text into the tool.[72] The PIMS will then attempt to present the information concerning the processing of personal data conducted by a specific controller in a more transparent way, either by re-organising and categorising it,[73] using icons or other visual means,[74] only presenting aspects relevant to the data subject,[75] or simply summarising the content.[76] Some even provide a rating for the privacy practices described within the policy.[77] While interpretative tools in general have the same aim there are, however, some differences in approaching such which might affect the role they take towards the data subject, which require consideration.

---

[71] *Hacker*, Datenprivatrecht, 567; *Pałka/Lippi*, in: Big Data Law, 115, 115ff; *Tesfay and others*, in: IWSPA '18, 15, 17; *Sadeh and others*, Usable Privacy Policy Project, 3f.

[72] *Harkous and others*, USENIX 2018, 531, 533-535; *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3; *Liepina and others*, in: ASAIL 2019, 1.

[73] *Harkous and others*, USENIX 2018, 531, 533-535.

[74] *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 2; *Harkous and others*, USENIX 2018, 531, 537f; *Tesfay and others*, in: IWSPA '18, 15, 19.

[75] *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3.

[76] *Tesfay and others*, in: IWSPA '18, 15, 19.

[77] *Harkous and others*, USENIX 2018, 531, 537f; *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3.

1. Standardised Translations

The most typical solutions both in existing tools and such under development, are standardised translations. Here, the developers decide on a form which they perceive as more comprehensible for the average person or target group and, based on that, re-represent all analysed privacy policies in that way. As mentioned previously, this might be achieved through the use of visual means such as icons, focus on certain crucial aspects of the processing, or simply a standardised reorganisation so that information can be found faster. The actual interests or needs of the individual are, however, neither asked for nor taken into account.

The functioning of such tools will typically not require the processing of any personal data. The analysed policies, while providing details with regards to processing activities conducted by other parties, will rarely include any personal information (other than maybe the contact details of the Data Protection Officer). It is also unlikely that any substantial amount of personal data of the user would be required for such an analysis. While there are some technical details which might be captured, such as for example the IP-address when using a web-based tool, or log-in details in cases where individuals set-up an account with the provider, this will be only very minimal. The interest of the provider to further process or use such data is also limited. Log-files are typically required for the optimisation of technical functionalities and content but are kept for very short periods of time and can be quickly anonymised. While the evaluation and anonymisation of such data would still be considered as processing under Art. 4 No. 2 and the provider would be the controller of such data, this does not go beyond the processing operations conducted by any other application or web-page and is not connected to the specific service offering of Personal Information Management Systems.

2. Personalised Translations

The result might, however, be quite different if a provider of a Personal Information Management System decided to make the presentation of the content of the policies more personalised. Whereas at the moment none of the tools reviewed under Part 1 Chapter 1: B. III. 1. Interpretative included such an option,[78] this might be considered a significant enhancement. It can be assumed that not all data subjects will be interested or concerned about the same aspects of the processing of their personal data. Some might be categorically opposed to the sharing of their data with third parties but have no reservations when it comes to the storage in third countries. Other might feel entirely different and be quite distrustful of any data transfers outside the EEA but not mind the sharing and further processing of such within its perimeters. Considering the sheer amount of information, a privacy notice needs to contain, it would make sense from the perspective of the PIMS provider to allow their individual users to simply set-up their preferences and only display elements relevant to them, thereby potentially reducing the cognitive load.

While, on the one hand, such solutions have the potential to even further eliminate the existing hindrances for the acquisition of transparent information, they will, on the other hand inadvertently cause a significant rise in processing operations on the side of the Personal Information Management Systems. Standardised translation does not require the collection of further processing of the user's personal data while as soon as a service offering is adjusted to the individual's preferences, these choices and selection will naturally relate to an identified or identifiable individual, categorising them "personal data" under Art. 4 No. 1. Depending on the extent of the functionality, these processing operations might also be quite extensive. Whereas a

---

[78]The Usable Privacy Project also conducts research on the modelling of privacy preferences, in order to determine which types of privacy disclosures are relevant in what context, including considerations of behavioural and cognitive biases (see: *Sadeh and others*, Usable Privacy Policy Project, 3f), at the moment however this does not seem to include attempts on adjusting the presentation of information for individual users.

basic preference set-up in which the user only requests to receive information about the storage period will not require any analysis of the data beyond a simple implementation of the individual's wishes, more elaborate or sophisticated designs are also imaginable. Data about their interests, priorities, and user behaviour can be used to further optimise the tool, develop strategies for other target groups, or simply enhance the individual's experience and thereby engagement with the application. After all, these types of techniques are already quite present in other areas, such as e-commerce or online marketing.

If, however, an application was to be installed locally without allowing any communication with the servers of the PIMS provider, controllership under the GDPR would be excluded in the same way as is the case with standard software products installed locally. While, on the one hand, this might be considered a more privacy friendly solution since the user's personal data never leaves their sphere of influence, it also potentially carries additional security concerns as the information might be more vulnerable than it would have been under the control of a system specialising in data security. The result, under which the potentially exact same functionality with the same possibilities and setting would be classified differently only based on the storage model (local or with the service provider), also seems a little problematic since a PIMS, even if installed locally, would establish how such a tool will be processing the preferences set-up by the user.

It should also be noted that while the analysed tools focus solely on the interpretation of privacy policies, actual Personal Information Management Systems, as envisaged by the EDPB and other actors, would likely include more functionalities also directed towards the potential sharing of data with other parties. In that sense, the deployment of more interconnected solutions is more likely in the future. For such, regardless of the extent to which such optimisation and personalisation are being performed, the provider of a Personal Information Management System would have to be considered a controller for such a processing operation. The application, including its

technical parameters, what kind of data is being captured, and when, is determined by the PIMS. The same applies to the purpose of the provided functionality. In effect, this means that, in the context of creating personalised translations of privacy policies, the Personal Information Management System therefore establishes the means and the purposes of the processing of personal data.

3. Recomendations

Another element which might be added onto the basic functionality of translating privacy policies, potentially affecting the roles taken by provider, is the inclusion of recommendations. These can, however, also come in varying forms and degrees. The most basic form of such is probably present in tools providing a rating for the privacy practices described within the policy, rather than just an objective presentation of the facts.[79] Following up on the idea of ratings is the successor of Polisis, PoliCompare, which is based on the same methodology but focuses on the comparison of data processing practices of multiple providers.[80] It allows users to select a maximum of 10 providers whose privacy policies are analysed by the application and then displayed in the form of a table, contrasting their guidelines against each other, as well as underlining positive and unfavourable aspects of each.[81] Going even further is the Competitor Analysis Tool (CAT), a component of Privacy Check introduced in 2020, which will display a chart comparing the privacy scored achieved by a particular company with those of other providers within the same market sector.[82] It also provides a list of the top three competitors which have achieved the highest scores with regard to GDPR compliance and

---

[79] *Harkous and others*, USENIX 2018, 531, 537f; *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3.

[80] Policompare, https://www.epfl.ch/labs/lsir/policompare/ (accessed: 20 October 2025).

[81] ibid.

[82] *Nokhbeh Zaeem and others*, WI-IAT 2020, 291, 291f.

user control.[83] The crucial difference between this tool and PoliCompare is that the users do not need to enter the URLs for the varying competitors. The application will independently provide the data subjects with alternative suggestions. Arguably going even further is the Usable Privacy Project in which the possibilities and methods of nudging users into making more privacy friendly choices are contemplated.[84]

The amount of personal data processed for the inclusion within such a functionality is essentially the same as in the context of the previously analysed standardised translations or possibly personalised translations if the recommendations were adjusted to specific user settings or preferences. What does, however, transpire is the formation of (a) a more significant impact on the user's decision-making process; and (b) a connection between the provider of Personal Information Management Systems and the controllers whose policies are being presented. Simply presenting statements within a privacy policy by means of standardised icons is one option but giving the data subject a specific rating and thereby suggesting whether their data will be secure with another party, is completely different. Here the presentation given by the tool can actively impact the individual's choices, either deterring them from using a certain service or confirming their choice. In that sense, the PIMS is actively impacting the intended processing of personal data in the form of influencing the decisions on whether the operation will even take place. This impact can still largely be attributed to the user's choice in the case of applications comparing the practices of companies defined by the data subject. Once the PIMS makes a specific recommendation of an alternative controller not previously considered by the individual, they are essentially creating the possibility for this alternative controller to collect and further process the user's personal data. The individual might still go against such a recommendation but the potential impact is undeniable.

---

[83] ibid 292.

[84] *Sadeh and others*, Usable Privacy Policy Project, 13.

Looking at the considerations of the CJEU in the case of *Fashion ID* where the court established the existence of joint controllership based on the fact that a webpage operator *"made it possible for Facebook"*[85] to collect visitor's personal data by embedding a plug-in and that they thereby exerted *"decisive influence over the collection and transmission of the personal data"*,[86] it needs to be asked how the influence of the PIMS is to be classified in that context. An individual might, for example, search for an alternative service provider potentially processing less personal data or in more secure manner than other businesses. The PIMS could provide them with a detailed comparison and potentially straight-forward recommendation on which company to choose. This essentially makes the collection of data by such possible and thereby exerts a decisive influence over the collection and transmission. This would be even more evident if the data subject was, for example, to be provided with a direct link to the web-pages of different companies. Furthermore, if the translation of privacy policies was to be paired with other service offerings, such as storage or consent management, the Personal Information Management System might even directly take over the transmission of the individual's personal data. If the determinations made by the Court of Justice of the European Union are therefore to be consequently followed, the conclusion needs to be reached that the provider of a Personal Information Management System which provides users with recommendations regarding the selection of service offerings by different controllers, is exerting decisive influence over the collection and transmission of personal data by that service provider and is thereby involved in the determination of the means of processing personal data.

The enabling of data collection alone is, however, not sufficient for the assumption of joint controllership as the PIMS and the potential controller would also have to be conducting a processing activity for joint purposes. This is hard to justify, considering that the purpose of a Personal Information Management System is, per definition, the

---

[85]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 75.
[86]ibid para 78.

empowerment of the individual, whereas it is impossible to pre-define the potential aims pursued by the recommended data controller, as these will depend on factors such as the sector in which they are active, their business model, or the types of services offered. Whatever these may be, it will therefore be unlikely that the purposes of these two entities might align. Again, however, a look at the rules established by the CJEU is necessary in this context. With regards to the determination of joint purposes in the case of *Fashion ID*, the court concluded that the *"processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland".*[87] Depending on the specific business model deployed by the Personal Information Management System, they could arguably also have an economic interest in the processing operation just like any service provider. Also, it is at least imaginable that if the potential controller which is being recommended by the PIMS, does in fact also pursue the aim of offering privacy friendly services, then the purposes of the different actors would also align and could potentially be considered as "joint" in the meaning of Art. 26(1). The dependency on the purposes of the PIMS and the recommended controller is, however, quite problematic since the determination of the roles of the parties, with regards to the processing activity, would depend on the underlying aims pursued by them, not just the objective functionalities of the service. This could potentially lead to an outcome where a PIMS would be considered a joint controller with one recommended company and as a separate controller regarding another, based on the business model of such.

The above considerations evidence how difficult the determination of the roles and responsibilities of the relevant parties is and how minimal changes in the technical offering, as well as pursued aims of the PIMS, have the potential to significantly affect their legal categorisation under the GDPR. It can however be concluded that taking

---

[87] ibid para 80.

into account the case law of the CJEU, Personal Information Management Systems, including a component which recommends certain companies based on their reported privacy practices, could potentially be considered as joint controllers in the meaning of Art. 26(1) of the General Data Protection Regulation.

II. Auditing

Auditing tools are intended to review privacy policies regarding their accuracy, as well as legal compliance.[88] This can either be done by comparing statements made by data controllers within their policies with the actual ongoing processing activity[89] or by means of reviewing the legality of the described practices.[90]

1. Standardised Audits

In principle, such a functionality does not require the processing of personal data on the side of the Personal Information Management System. In the sense of the roles taken by the application vis-a-vis the data subject, the review of the legality of the suggested terms with the provisions of the GDPR, is essentially identical to that taken by providers of interpretative tools offering standardised translations. Some technical details, such as for example the IP-addresses when using a web-based tool or log-in details in cases where an individual has set-up an account with the provider, might still be captured. Their extent will, however, only be minimal and qualified as a standard separate controllership, which does not relate to the specific service offering.

The same will generally apply when considering the two analysis tools MAPS and AppTrans, which compare the disclosures made by

---

[88]See Part 1 Chapter 1: B. III. 2. Auditing.

[89]See for example: *Zimmeck and others*, PoPETs 2019, 66, 67; *Austin and others*, Towards Dynamic Transparency, 15f.

[90]See for example: *Contissa and others*, CLAUDETTE meets GDPR, 15.

app providers regarding the processing of personal data being conducted, with the behaviour of the application based on their code.[91] Here, no personal data of the users is processed. While these two specific solutions have not been created with data subjects as primary users in mind but rather in order to support regulatory agencies and app store providers,[92] they evidence that no personal data would need to be processed when offering such a service to an individual. In that sense, the provider would not take any specific function under the GDPR in the context of the service offering.

2. Personalised Audits

An interesting consideration would, however, be the possibility of reviewing the processing conducted by an application of one's own personal data, with the declared privacy practices of a company. As outlined under Part 1 Chapter 2: B. III. 2. d) Reductive Potential, the main advantage of auditing tools for the data subject lies in supporting them in taking further action against an incompliant controller. This could, for example, be done in the form of issuing a complaint with the Data Protection Authority under Art. 77 or claiming damages under Art. 82. These claims, however, require either the materialisation of damages on the side of the individual, or the belief of such that the processing of personal data *"relating to him or her"* is infringing the Regulation. In that sense, it would arguably be necessary to prove an actual effect on the data subject, whereas a generalised statement on the illegality of the controller's practices might not suffice. Therefore, in order for a Personal Information Management System to actually "empower" the individual to issue such claims, the tool would ideally be able to provide evidence of misconduct on the specific dataset.

---

[91] *Zimmeck and others*, PoPETs 2019, 66, 72-74; *Austin and others*, Towards Dynamic Transparency, 15f.

[92] *Zimmeck and others*, PoPETs 2019, 66, 80; *Austin and others*, Towards Dynamic Transparency, 9f.

If the functionality was to be extended that far as to allow the analysis of the processing conducted on the individual user's personal data, then inadvertently the PIMS would also need to process these data points. Considering the fact that the PIMS would then be conducting processing operations on the exact dataset processed by the controller, the question of joint controllership might arise. Such an outcome would, however, not be possible. While the broad interpretation of "joint purposes" established by the CJEU might allow such a consideration in many cases, it will clearly not work here, as the interests of the Personal Information Management System and the controller processing personal data are contradicting themselves, rather than being mutual in any form. The PIMS is essentially used to prove misconduct on the controller's side, thereby going against whatever purpose they were trying to achieve. In that sense, a Personal Information Management System offering the functionality of auditing the processing activity of controllers, with regards to a specific dataset, will also be qualified as controllers under Art. 4 No. 7 of the GDPR, however, in an entirely separate capacity from the examined business.

III. Responsive

As discussed under Part 1 Chapter 2: B. III. 3. Responsive, these tools are not necessarily to be seen as a separate type altogether but rather as a subcategory of interpretative and auditing functionalities, as they do not differ from these two in connection to their goals but rather the presentation of the achieved results. Instead of using the standard form or presentation, the information is displayed to the user in the form of a "response" either to a specific question or concern, thereby seemingly making the experience more interactive on the user's side. The two analysed examples are PriBot,[93] an automated chatbot answering free-form questions about privacy policies, and PrivacyBird,[94] a Browser-Helper-Object (BHO), which provides

---

[93] *Harkous and others*, SOUPS 2016, 1.

[94] Privacy Bird, http://www.privacybird.org/ (accessed: 16 October 2025).

users with a determination on whether or not the currently used website matches their personal privacy preferences.

While the basic functioning is similar to that as described in other tools, essentially translating the controller's policy into a more comprehensible form, the communicational element of these makes them closer to a personalised translation, rather than a standardised one. Here the necessity to process personal data is, however, even stronger than before. While personalised translations might have theoretically worked through local installations without any communication with the PIMS itself, this is very unlikely to work in the case of tools intended to simulate a form of communication with the user. For Chatbots to properly function and actually provide useful answers to the individual, users feedback needs to be collected and processed.[95] While an offline solution might therefore constitute a nice gimmick, it is unlikely to be able to mimic an actual interactive experience. Also, considering the latest rise in the development of generative AI models such as Chat GPT or Google Gemini, users will by now be expecting a high-quality experience when interacting with a responsive tool. In fact, AI might be used to significantly enhance the currently existing landscape of Personal Information Management Systems. Considerations on AI systems and the influence of the AI Act will, however, be discussed at a later stage, in Part 3 of this thesis (see Part 3 Chapter 6: F. AI-Act). At this point, it should only be emphasised that where a tool utilises the individual's responses, both for the purpose of the current interaction as well as future optimisation, the provider of a Personal Information Management System would have to be considered a controller for such a processing operation, as they are determining the technical parameters and the type of data being captured, as well as the form in which it is being analysed.

---

[95] *Harkous and others*, SOUPS 2016, 5.

IV. Interim Conclusions: Information

Both in the case of standardised translations and standardised audits, no personal data would need to be processed as part of the service offering itself, which means that in that context the provider of a Personal Information Management System would not take any roles under the GDPR, vis-a-vis the data subject.

Where, on the other hand translations or audits are being personalised, the functionality is likely to require the processing of personal data, for which the PIMS would establish both means and purposes, thereby rendering them controllers in the meaning of Art. 4 No. 7. In the case of interpretative tools this is based on the consideration that they would respond to a specific user concern or set-up, which inadvertently relates to them. For auditing functionalities, the idea would be to analyse the processing conducted on the individual user's personal data by other controllers for the purpose of evidencing a misconduct on their part and allowing the issuing of complaints or claims for damages under Articles 77 and 82, respectively. For the implementation of such a function, the PIMS would inadvertently have to process the same data points as the audited entity. This would, however, be conducted for different purposes, making them a separate controller.

The same essentially applies in the case of responsive tools, which display the information relevant to the user in the form of a "response" in order to create a more interactive experience. Here the extent of the processing of personal data required for a proper working of such a functionality is likely to be even greater, since the utilisation of the individual's responses, both for the purpose of the current interaction as well as future optimisation, will likely be necessary in order to assure the proper functioning of such tools.

The most problematic applications in the context of attributing an appropriate role under the General Data Protection Regulation are transparency enhancing tools which provide the end user with recommendations regarding their selection of service providers. Taking into account the broad interpretation of joint controllership established by the CJEU case law under which economic interests on the side of the parties might already count as a joint purpose and the

creation of a possibility for another controller to collect personal data is rendered as *"decisive influence"* over the means of processing, it can at least be argued that systems with such a functionality would need to be considered joint controllers within the meaning of Art. 26 GDPR.

C. Consent

As has been outlined under Part 1 Chapter 2: C. Consent, a number *of* Personal Information Management Systems offering a functionality of consent management have been developed. These mainly aim at solving the many identified obstacles in the collection of truly valid consent such as heuristics, cognitive, and behavioural biases, as well as consent fatigue. It has been concluded that the reviewed service offerings can be considered as an important step in improving the current landscape but are still subject to many limitations. In that sense, both the legal designation of the existing offerings, as well as that for potential future and more efficient solutions will be considered below.

I. Existing Service Offerings

The existing service offerings vary on many levels such as in their maturity status and technical approach to managing consent, as well as opinions on the legal role they should take with regards to the data subject. The positions of Meeco and MyDex, which also include consent management as part of their functionalities, have already been discussed in the context of storage (see Part 2 Chapter 4: A. II. 3. b) Meeco and d) Mydex). In that sense, a reminder should be sufficient at this point that Meeco essentially qualified themselves as a processor with regards to their main service offering, whereas MyDex is

established as the "owner and controller of the data architecture of Mydex Master PDS Data Schema".[96]

1. Plus Privacy

The application "Plus Privacy" was created as part of the OPERANDO[97] research project and provides data subjects with a unified dashboard, allowing control over privacy settings in social media accounts.[98] Currently, data subjects are given the option to configure all data privacy settings on Google, Facebook, X, and LinkedIn at once, while also retaining the option to adjust those individually.[99] According to their privacy policy, the Plus Privacy application can be used anonymously without providing any personal or device information, as long as the individual is not logged in.[100] Conversely, using the platform in combination with a user-account or in the context of the described "opt-in" e-mail identity management does require the processing of personal data.[101] Unfortunately, the provider's privacy policy does not explicitly mention the role they play in the processing operation. From the available text it can, however, be deduced that the provider considers themselves a controller, separate from the end recipients Google, Facebook, X and LinkedIn only with regards to the account related data and the available opt-in services, but not beyond that.[102]

---

[96]Mydex Charter, https://dev.mydex.org/mydex-charter.html, (accessed: 20 October 2025).

[97]Online Privacy Enforcement, Rights Assurance and Optimization, https://cordis.europa.eu/project/id/653704 (accessed: 20 October 2025).

[98]Plus Privacy, https://plusprivacy.com/ (accessed: 20 October 2025).

[99]Plus Privacy FAQ, https://plusprivacy.com/faq/ (accessed: 20 October 2025).

[100]Plus Privacy Privacy Policy, https://plusprivacy.com/privacy-policy/, (accessed: 20 October 2025).

[101]ibid.

[102]ibid.

2. World Data Exchange

World Data Exchange offers both a consent and data portability feature. Users are able to receive data from their "data sources" in JSON format, as well as share it further with other enterprises.[103] The consent feature is intended to allow the collection of explicit and informed user consent by laying down all relevant information in a clear manner via a standardised consent screen.[104] The privacy policy currently found on the website only applies to processing operations conducted while visiting the website and does not refer to those connected to the actual service.[105] An older version, reviewed in February 2023, while the application was still called (Digi.me)[106] did however go into the question of controllership to a certain extent. For example, in England where individuals who use their National Health Services login details in order to access the service, it clearly stated that Digi.me is to be regarded as a processor as they "must act under the instructions provided by NHS Digital".[107] Controllership was also evidently excepted for data processing in contexts such as: signing up for newsletters; signing up as a beta user or tester; submissions of bug reports via Instabug; the completion of forms on the website; entering competitions or surveys; attendance of hackathons; contact via e-mail, phone, post or social media; or employment applications.[108] With regards to the tool itself or specifically the consent fea-

---

[103]World Data Exchange Features, https://worlddataexchange.com/features (accessed: 20 October 2025).

[104]ibid.

[105]World Data Exchange Privacy Policy, https://worlddataexchange.com/privacy-policy (accessed: 20 October 2025).

[106]This name is now used for a different, more specific application offered by World Data Exchange, focused on health data management. See: https://digi.me/ (accessed: 20 October 2025).

[107]Digi.me Privacy Policy, https://digi.me/privacy-policy (accessed: 20 October 2025).

[108]ibid.

ture nothing is, however, explicitly mentioned. It can therefore be assumed that World Data Exchange does not consider itself to be a "controller".
Since the functioning of the application is largely dependent on data controllers cooperating with the service, its marketing is also largely directed towards businesses. The website, for example advertises that they are "[t]he right way to get explicit and informed consent from your users to use their data".[109] This would in a sense suggest that they might in fact take the role of processor for the end recipient who is interested in the user's personal data. The processing operation that is being commissioned would then be the collection of valid consent on behalf of the controller. This, however, is not stated at any point and would also in a sense go against the purpose of PIMS, which is the empowerment of the individual.

3. Advanced Data Protection Control

Advanced Data Protection Control (ADPC) works through the exchange of HTTP headers between the data subject and the relevant web server[110] and is primarily intended to remedy the current way of collecting personal data through the use of "cookie banners".[111] As of the time of writing, the platform was, however, not yet functioning and only a prototype was available for review.[112] With regards to such, the ADPC privacy policy did, however, clearly state that the "*plug-in stores all your data locally within your browser, so you are*

---

[109]World Data Exchange Features, https://worlddataexchange.com/features (accessed: 20 October 2025).

[110] 'Advanced Data Protection Control (ADPC) - Unofficial Draft 08 July 2021', https://www.dataprotectioncontrol.org/spec/#concept (accessed: 20 October 2025)..

[111]Advanced Data Protection Control, https://www.dataprotectioncontrol.org/ (accessed: 20 October 2025).

[112]ADPC Implementation Prototype ,https://www.dataprotectioncontrol.org/prototype/ (accessed: 20 October 2025).

the 'controller' for your personal data when using this software".[113] Since "controller" is written in quotation marks and there is no actual reference to an Article in the GDPR, it is not entirely clear whether the data subject is considered as a controller in the meaning of Art. 4 No. 7, or just as "in control" of their information and with whom they share it. What is evident, however, is that the ADPC does not consider itself either a controller or processor with regards to the provided consent management functionality. The privacy policy goes on to clarify that there are no guarantees as to the actual functioning of the initial prototype but that all data is being stored locally and not reported back to any parties.[114] While the project does not make any statements regarding the future division of responsibilities between the parties, it can be assumed that they are likely to apply the same classification in the future. Similarly, as with other providers, ADPC points out on multiple occasions that no personal data of the user is being stored by them as part of the provision of service.[115] Based on that, the conclusion seems to be that they are a third party and not a controller or processor under the GDPR definition.

II. Legal Classification

Looking at the information contained within the privacy policies of the analysed providers, it can be concluded that none of them have qualified themselves as controllers with regards to the functionality

---

[113]ADPC Privacy Policy, https://www.dataprotectioncontrol.org/privacy-policy/ (accessed: 20 October 2025).

[114]ibid.

[115]For example: "*When you give a permission to dataprotectioncontrol.org via ADPC we do not actually use your personal data, but just alter the test page to give you an idea how different types of advertisement may be shown to a user depending on the ADPC signals sent to the website*." See: ADPC Privacy Policy, https://www.dataprotectioncontrol.org/privacy-policy/ (accessed: 20 October 2025).

of consent management. While some accepted responsibility as processors, for certain parts of the service, or at least implied this, [116] most seem to assume that they would need to be considered as third parties under the GDPR. [117] While the determinations made by the parties may be taken into account, they are still subject to review. It has been established that the legal designation of the parties is based on their actual influence and activities regarding the processing of personal data and may not be altered through formal designations contradicting the factual circumstances.[118] Also, as mentioned previously, while the currently available tools are certainly quite relevant in furthering the future of effective consent management, improvements are still to be expected. Changes are therefore likely to occur within the technical infrastructure. Therefore, the considerations on the roles and responsibilities should be kept more generalised, rather than connected to a specific service offering.

As has been established in the beginning of this Part, all the legal terms under the GDPR are functional concepts and need to be interpreted taking into account the overall circumstances of the processing of personal data and according to the actual activities taken by the parties in a specific situation (see Part 2 Chapter 3: A. IV. Functional Element). This has also been the case when analysing the previous two functionalities of storage and transparency. The focus of these, however, was always on the relationship of the PIMS with the data subject whereas in the case of consent, the presence of another actor who is likely to be considered a controller in relation to the individual providing their personal data, also needs to be accounted for. Considering the various forms in which consent may be

---

[116]Digi.me Privacy Policy, https://digi.me/privacy-policy (accessed 3 February 2023).

[117]ADPC Privacy Policy, https://www.dataprotectioncontrol.org/privacy-policy/ (accessed 24 October 2025); Plus Privacy Privacy Policy, https://plusprivacy.com/privacy-policy/ (accessed 15 January 2025).

[118]*Bassini*, BLP 2019, 103, 107f; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 148; *EDPB*, Guidelines 07/2020, para 12; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 88; *Berger/Eisendle*, 15 IJLT 2019, 20, 24.

managed, focus should therefore be put on both the technical aspects, as well as the relationship between the parties.

1. Relevant Processing Activity

The role taken towards the data subject will always need to relate to a specific processing activity. While an IT-Service provider will typically be considered a processor with regards to the personal data of its customers, it will still retain the position of controller for all processing operations related to its own employees. Since Personal Information Management Systems are put in place precisely so that individuals can gain more control over the processing of their personal data, it is particularly crucial to clearly define for which processing operation a specific assessment is being made. This determination was more or less straightforward with the other two functionalities of storage and providing transparent information. In the case of consent management there are, however, two elements which need to be clearly separated from each other: the intended processing activity for which consent is being obtained and the activities taking place in the preceding stages, connected to the collection and transmission of the users' personal data.

a) Intended Processing Activity

The purpose of the PIMS is the collection of valid, freely given, specific, informed, and unambiguous consent from a natural person for the processing of their personal data in order to create a valid legal basis for such under Art. 6(1)(a) or 9(2)(a) in the GDPR. This consent is being obtained for another entity which is interested in this information and intends to process it for their own purposes. There is no limit as to what these may constitute from market research, the supplying of goods, social media channels, health management, financial services and so on and so forth. It can also clearly be assumed that such an entity will be considered the controller with regards to that processing activity, as it is establishing both the means and purposes of the processing of personal data. What is not clear,

on the other hand, is how the operations of the Personal Information Management System are to be classified in that context.

aa) Processor

While the PIMS provider has no underlying interest in using the data subjects' personal data for their own purposes, nor do they attempt to reach a common goal with the receiving entity, they are essentially providing such with a valid legal basis for conducting their operations. In that sense, they might be considered as processors of the end recipient. This position can partially be observed in the context of The Wold Data Exchanges old Privacy Policy, which openly confirmed its position as a processor with regards to NHS login details.[119] Additionally the provider markets itself as supporting controllers in obtaining explicit and informed consent on behalf of the business customer.[120] The same approach has also been taken in the context of Consent Management Platforms under the IAB Europe Transparency & Consent Framework, which clearly designates them as processors for the Publishers.[121]

This also largely makes sense since the assurance that the consent received from the data subject is meeting the requirements of the GDPR, the ePrivacy Directive, or other relevant legislation is after all in the interest of the party intending to process the users' personal data. There are, however, two issues which require consideration. First of all, even in the case of Consent Management Platforms acting solely on behalf of the end recipient, such as those considered in the IAB Europe Transparency & Consent Framework, there are instances in which the classification as a processor is possibly inaccurate and they might be considered as controllers after all.[122] This is,

---

[119]Digi.me Privacy Policy, https://digi.me/privacy-policy (accessed: 3 February 2023).

[120]World Data Exchange Features, https://worlddataexchange.com/features (accessed: 22 October 2024).

[121]https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf (accessed: 04 March 2026).

[122]*Santos and others*, in: Privacy Technologies and Policy, 47, 54-63.

for example, the case when additional processing activities are included in the tool, when scanning or pre-sorting of tracking technologies is being performed, when third-party vendors are included by default, or interfaces with manipulative design strategies are being deployed.[123]

Secondly, the consideration of a Personal Information Management System as a processor is in a sense incompatible with its purpose. As has been established in Part 1 Chapter 1: A. I. Compliance Management, a number of varying compliance tools has been developed as a result of the GDPR coming into force.[124] While these are also frequently described as "PIMS" and often include quite similar functionalities with correlating goals, their primary focus is the support of the controller in adhering to the legal requirements to which they are subject, not the support of the individual. The types of tools analysed as a subject of this thesis are, on the other hand, "technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data",[125] thereby excluding service offerings focused on the controller's interest. In that sense, consent management platforms which are truly acting on behalf of another entity and based on their documented instructions, as would be required for a processor, should per se be excluded from the definition of Personal Information Management Systems in the meaning applied in this thesis.

Nonetheless, this exclusion leads to an interesting conundrum. As has been evidenced in the analysis of current consent management functionalities on the market (see Part 1 Chapter 2: C. V. Interim Conclusions: Consent*),* the solutions which can be considered most mature from a commercial perspective, such as World Data Exchange, MyDex and Meeco, are largely dependent on a cooperation with the end recipient of the data in order to assure their proper func-

---

[123] *Santos and others*, in: Privacy Technologies and Policy, 47, 67.
[124] *Jung*, 5 ZD 2018, 208, 208ff.
[125] *EDPS*, Opinion 9/2016, para 4.

tioning. It is, after all, logical that the Platform would need to cooperate with the controllers in some form in order to properly work and therefore provide any sort of added value for the data subject. If, on the other hand, a platform wants to convince controllers to collect consent through them, some sort of benefit would probably need to be advertised to these as well. In that sense, the creation of a truly, solely user-centric PIMS is likely to have reached its limits. Another practical consideration which should be taken into account is the fact that if the connection between the PIMS and the controller was per definition denied, then, unless the PIMS was to be defined as a controller as well, they would not be subject to any responsibility under the GDPR, leaving the data subject without any actions of recourse against them.

bb) Controller

It should therefore be considered to what extent the Personal Information Management System could be qualified as a controller under Art. 4 No. 7. Such a classification might in fact seem reasonable when looking at the findings of the CJEU in the context of Fashion ID. Here the court decided that the parties should be considered as joint controllers based on that fact that the website operator "made it possible for Facebook Ireland to obtain personal data of visitors".[126] The same can, after all, be said about any consent management platform, regardless of how it operates, as it essentially opens up the possibility of further processing for the recipient.

There are, however, some crucial differences between the two scenarios which should be taken into account. First of all, joint controllership not only requires a cooperation when it comes to the means of processing personal data but most importantly a common purpose in the processing activity. Whereas in the case of the website operator and Facebook a joint economic interest could arguably be established based on the fact that Fashion ID was in fact also

---

[126]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 75.

interested in gaining commercial advantages "consisting in increased publicity for its goods",[127] the same cannot be assumed for the PIMS. The provider of a consent management platform might also have a commercial interest in providing the service but such an interest is not connected to the intended processing activity which can be replaced with any other processing by any other controller. Unlike Fashion ID, a consent management platform will make no selection for the data subject with regards to the recipients of their data, but will rather be interested in offering the widest possible choice in services. Furthermore, the CJEU clearly recognises such a differentiation by excluding Fashion ID from any subsequent processing operations performed after the initial data transmission.[128] It would therefore contradict basic logic to attempt to extend the responsibility of the PIMS over the intended end processing activities, for which consent is being obtained.

b) Collection and Transmission

While therefore responsibility for the intended processing activity cannot be concluded for the consent management platform, its relation in the preceding stages of such should still be examined.

aa) Of Datasets

A Personal Information Management Platform also offering secure storage services is likely to be actively involved in the collection and transmission of personal data to the end recipient when providing consent management as part of their services. In that sense, they would be establishing means and purposes of this processing stage as they are providing a secure channel for the transfer of the users' data. This service offering should also be considered separately from the storage services themselves, as the provision of a secure transfer channel by means of encryption and other security measures can

---

[127] ibid para 80.
[128] ibid para 76.

be relevant regardless of the form in which data is being stored and will therefore be applicable equally in the context of local, as well as cloud-based storage. Such an understanding would also be in line with the discussed CJEU case law, which clearly allows the divisions of processing activities into separate stages.[129]

While it is therefore clear that the PIMS must be considered a controller for the transmission of a user's dataset, vis-a-vis the data subject; if this is part of the requested services, the question occurs how the relation between the PIMS and the recipient is to be classified. On the one hand, this could be classified as a separate controllership in which the Personal Information Management System is simply being commissioned by the data subject to transfer personal data from one place to another, the PIMS and the recipient have no common interests, and the PIMS is liable for any potential breaches or technical difficulties which might arise as a result of the transfer.

This line of argumentation is, however, unlikely to work in the case of a PIMS cooperating with end recipients. At the moment, the most commercially viable platforms allowing the management of consent, access, transfers and portability to a multitude of providers all operate based on a cooperation with the providers themselves, which also sign up to the intermediary service.[130] This means that there is an active collaboration between the platform and the controller receiving the data for their own purposes. It can therefore be assumed that the party acquiring a set of personal data based on the user's consent and collected via the PIMS will also have an active interest in having such transmitted in a secure manner. Also, by selecting to sign-up with the intermediary platform, they are affecting how the consent will be collected from the data subject and who will be responsible for that process, thereby establishing the means of such processing. In a sense, this can be seen as a reversal of the roles

---

[129]Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551, para 66; Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 70.

[130]See for example: Meeco, https://docs.meeco.me/platform/tenants-organisations-and-end-users (accessed: 24 October 2024); MyDex, https://mydex.org/platform-services/#mrd (accessed: 24 October 2024).

assigned in Fashion ID and Wirtschaftsakademie, where the fan page and website operator decided on the channels through which their content should be promoted. In the case of PIMS, where a controller decides to sign-up for the use of an intermediary service, they are thereby making the same type of selection, deciding which channel to use for the collection and transmission of the personal data of their end users. Based on that it, should be assumed that the Personal Information Management System and the controllers which have signed up on their platform should be considered joint controllers for the transfer of personal data conducted by the platform.

bb) Of Consent

While controllership, either separate or joint, can easily be established for the transmission of personal data to another party conducted by the Personal Information Management System on behalf of the data subject, cases where such transfers are not part of the service offering should also be considered. There will be instances in which a platform focuses solely on the collection of consent and the transmission of such to the end recipient without actually transferring the information intended for further processing. This will most likely be the case where no additional service such as the storage or portability of data is offered. A combination with a simple interpretative or auditing functionality is also imaginable but since these do not trigger any sort of legal responsibility under the GDPR unless they are personalised, this would have no effect on the role of the PIMS.

(1) Consent as Personal Data

What should, however, be analysed is the role taken by the PIMS with regard to the transmission of the consent signal itself. In accordance with Art. 4 No. 11, consent means “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. The data regarding the individual’s consent, transmitted to

the controller, therefore contains their wishes and information as to the processing to which they have agreed. This information can ultimately be considered as relating to an identified or identifiable natural person. After all, the requirements for consent to be specific, informed, and unambiguous make it necessary to capture who has provided their agreement and even under which circumstances. In consequence, the consent itself will also need to be qualified as personal data. This means that the provider of a Personal Information Management System will be responsible for the collection and transmission of personal data, regardless of whether or not the other datasets intended for processing are also transferred by them, as the collection and transmission of consent itself already constitutes a processing activity.

(2) Seperation of Consent

While handling consent notices does constitute processing of personal data, it should, however, be questioned to what extent this can in fact be considered a separate activity from the intended final processing operation, or whether these are not inextricably linked. Although the CJEU case law did introduce a fragmented approach to processing, allowing controllership for specific stages independent of the subsequent activities, in the case of Fashion ID there was, after all, a transfer of additional user data, not just the legal basis itself. On the other hand, the gathering, organisation and further submission of the user's preferences constitute the core activity of a consent management platform and will, in fact, be executed independently from the further actions taken by other controllers. If, after all, a user did not agree to certain practices or requested the blocking of data collection, this would also need to be captured in the tool. Such a "lack of consent" would be just as personal as the consent itself.

A "separation of consent" in this manner can also typically be observed in areas such as market research or clinical trials. Here it is, after all, not uncommon for the interested party to hire a provider responsible for recruiting participants, either directly or through their

databases.[131] These providers will also typically qualify themselves as "controllers" in the context of participant recruitment and consent management, especially if the individual's data is not just collected for one specific project.[132] The practice of considering the management of the data subjects' consent as a processing activity which can be viewed separately from the activity for which it is being provided, thereby seems to be commonly accepted. Based on that and taking into account the fact that the collection, organisation, and further transmission of the user's privacy choices constitutes the core functionality of a consent management platform, it should be assumed that the PIMS is establishing both the means and the purposes for the processing of such personal data and can thereby be qualified as a controller.

(3) Relation to the Recipient

The qualification of the Personal Information Management System as a controller for the collection, management, and transmission of a

---

[131]See for example: FieldworkHub International, https://fieldworkhub.com/market-research-recruitment/ (accessed: 24 October 2025); Silk&Otter Research, https://silkotter-research.de/en/market-research-recruitment-agency-germany (accessed: 24 October 2025); IQVIA, https://www.iqvia.com/solutions/research-and-development/clinical-trials/patient-recruitment (accessed: 24 October 2025); Trialbee, https://trialbee.com/patient-recruitment/ (accessed: 24 October 2025).

[132]See: FieldworkHub International Respondent Personal Information Policy, https://fieldworkhub.com/respondent-personal-information-policy/ (accessed: 24 October 2025); Silk&Otter Research Data Protection Statement, https://silkotter-research.de/en/privacy-policy (accessed: 24 October 2025); Krämer Marktforschung Data Privacy Statement, https://www.kraemer-germany.com/en/contact/data-protection/ (accessed: 24 October 2025); IQVIA Privacy Policy, https://www.iqvia.com/about-us/privacy/privacy-policy (accessed: 24 October 2025); Trialbee does not make their Privacy Policy in connection to the sign-up for clinical trials publicly available, but since the provider states that the information is being made available when registering for an account, it can be assumed that they also consider themselves responsible in that regard. Trialbee Privacy Policy, https://trialbee.com/privacy/ (accessed: 24 October 2025).

consent signal again raises the question as to whether or not this should be qualified as a joint or separate controllership from the end recipient conducting the processing activity, for which the consent is being given. In this context, the previous considerations regarding the collection and transmission of data (see Part 2 Chapter 4: C. II. 1. b) aa) Of Datasets) can largely be referred, as the same rule may be applied here as well. Where the PIMS is solely communicating and acting upon the wishes of the data subject without any involvement or even knowledge of the recipient, the tool should be qualified as a separate controller. If on the other hand the PIMS is set up in a way that requires the sign-up of (potential) controllers, as well as the data subject, the recipient will have a decisive influence on the processing operation by means of selecting the intermediary and should therefore be qualified as a joint controller for the consent management functionality.

2. Determination

Once the relevant processing of personal data with regards to which the Personal Information Management System should be taking a role is established, the question as to who determines the means and purposes for such needs to be considered. As outlined in the beginning of this section,[133] "determination" means "the process of deciding something officially"[134] and thereby requires a decision-making power with regards to the processing activity.[135] While the exerted influence of the PIMS over the operations has already largely been discussed in the context of each of the relevant processing activities, there are two aspects which concern all of these instances but have so far been left aside, namely access to personal data and the relationship with the individual. These will therefore be analysed in the following text.

---

[133] See Part 2 Chapter 1: A. II. 1. Determination.

[134] Oxford Learners Dictionaries, https://www.oxfordlearnersdictionaries.com/definition/academic/determination (accessed: 24 October 2025).

[135] *EDPB*, Guidelines 07/2020, para 19; *Voigt/von dem Bussche*, GDPR, 19; Sydow/Marsch / *Raschauer*, Art. 4, para 123.

a) Access

Many providers of Personal Information Management are operating on a "zero-knowledge" policy, by which the PIMS itself does not access the individual's personal data, nor processes it for their own purposes.[136] Based on that, it is frequently assumed and argued that this essentially qualifies them as a third-party intermediary, rather than a controller and a processor under the GDPR.[137] This conclusion is, however, neither in line with the formal definition of controllership, nor the essential guidelines available in the field. While a processor who per definition "processes personal data on behalf of the controller" (Art. 4 No. 8 GDPR) would need to either have access to personal data or at least have oversight and supervision of automated processing operations within their infrastructure, such active involvement is at no point required from the controller. The focus here lies in the element of determination and therefore an authority over decisions made with regards to processing and not at all in relation to actual physical access.[138] This is also explicitly confirmed in the EDPB Guidelines, which state in the executive summary that it "is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller".[139] There is

---

[136] *European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016) 11; Mydex, Achieving Transformation at Scale, https://mydex.org/resources/papers/AchievingTransformationAtScale/ (accessed: 24 October 2025).

[137] For example, the following providers truly underlined this fact, in order to argue their lack of responsibility: PlusPrivacy, https://web.archive.org/web/20240222035009/https://plusprivacy.com/privacy-policy/ (accessed: 24 October 2025); ADPC Privacy Policy, https://www.dataprotectioncontrol.org/privacy-policy/ (accessed: 24 October 2025). The same approach used to be taken by DigiMe, however, during the time of writing they have amended their Privacy Policy: DigiMe Privacy Policy, https://digi.me/privacy-policy (accessed: 24 October 2025) and now seem to accept controllership.

[138] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 7 DSGVO, para 20.

[139] *EDPB*, Guidelines 07/2020, para 3.

also no conflict nor commonly expressed contrary opinions voiced either by practitioners, literature, or case law. In that sense, any sort of exclusion of controllership based on the argument that the Personal Information Management System is not accessing the personal data for other purposes than the essential service offering, should be categorically rejected. Their roles and responsibilities should rather be determined based on their influence over the processing of personal data, in the context of each relevant element of the service offering, as already established in this thesis.

b) Perspective of the Data Subject

Another aspect which should at least be taken into account when establishing the rights and responsibilities in the context of a Personal Information Management System is the perspective of the data subject. On the one hand, the roles of controllers and processors are all functional concepts and are therefore to be decided based on the actual factual influence of the entities.[140] On the other hand, however, the principles of lawfulness, fairness, and transparency enshrined in Art. 5(1)(a) of the GDPR also clearly introduce an obligation to take the perspective of the affected individual into account.

The primary focus lies on the transparent provision of all relevant information which needs to be easily accessible and easy to understand, as underlined by Recital 39. The idea of "fairness", however, also includes the requirement that personal data should not be processed in a form which cannot be reasonably expected by the data subject, even if that information has arguably been laid down in a transparent manner.[141] This should logically also include the question of the division of responsibilities between the actors visible to the affected individual and can in a sense be derived from the information requirements under 13(1)(e), 14(1)(e), and 26(2), all of which

---

[140]Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 148; *EDPB*, Guidelines 07/2020, para 26f; *Bassini*, BLP 2019, 103, 108.

[141]Ehmann/Selmayr / *Heberlein*, Art. 5, para 14 *Roßnagel* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 5 DSGVO, para 47.

essentially strive to allow the data subject to understand which parties are involved in the processing of their personal data. In the context of consent management, the PIMS is the primary actor with whom the individual will be interacting; they are likely to be the stakeholder that provides all relevant information regarding the planned processing activity and collecting the consent. While further processing will not be conducted by them, they are certainly at the forefront and arguably the entity in which the data subject puts their trust. While this should therefore not be considered the decisive element when determining the respective rights and responsibilities of the involved parties, the perspective of the data subject, when and how they interact with the parties and what their reasonable expectations in consideration of the circumstances might be, should also be accounted for.

III. Transparency

The question of transparency is relevant for Personal Information Management Systems on multiple levels. First, when the functionality of the system uses transparency enhancing technologies which are part of the relevant service offering. Second, where the platform includes the possibility of consent management, since the requirement of consent to be informed also includes the obligation to provide the individual with transparent information concerning the processing operation.[142] And finally in the context of transparently presenting all relevant facts concerning the processing operations performed by the platform or as a result of the provided services, and how the rights and responsibilities of the involved parties are divided for such. The first two points—the current hindrances in providing transparent information and obtaining valid consent, as well as the forms in which

---

[142] *Klement* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO, para 72; Kuner and others / *Bygrave/Tosoni*, Art. 4(11), 174, 183f; Kühling/Buchner / *Hartung*, Art. 4 Nr. 11 DSGVO, para 8; Paal/Pauly / *Ernst*, Art. 4 DSGVO, para 79.

these goals can be achieved by the PIMS—have been discussed at length in Part 1 Chapter 2: A. Information and C. Consent and can therefore be left aside here.

1. Processing

When considering the preceding analysis of the respective roles taken by a Personal Information Management System with regards to the functionality of consent management, it becomes evident that its legal designation depends on a number of factors. The two most relevant can generally be described as: (1) the extent of the service offering; and (2) the relationship with the recipient. When it comes to the first, the provisions of transparent information should be reasonably achievable. The data subject should likely be aware whether or not they have uploaded their data onto the platform and or had it transferred automatically, or whether they have to do so on their own within the infrastructure of another controller. Information on whether or not the PIMS has access to the relevant data, under which circumstances, and for what purposes would also generally be included in the standard service agreement concluded with the platform. Where an individual decides to acquire the services of a provider of Personal Information Management, they are likely to have considered the possible functionalities offered to them in advance. While the details concerning the processing of personal data within the tool would still need to be presented transparently in a privacy policy, it can be assumed that the affected individual should be generally aware of the performed conduct.

2. Relationship

The same, however, cannot be said regarding the relationship between the PIMS and the end recipient of the data. As has been discussed previously in the context of responsibility for the intended processing activity for which consent is being obtained *(*see Part 2 Chapter 4: C. II. 1. a) Intended Activity), a Personal Information Management System will generally not take any role with respect to such, as they are not involved in the determination of means and purposes,

and instances in which they are acting on behalf of the main controller where they might be considered as processors would in principle exclude them from the definition of PIMS. While this differentiation between the business model of a specific platform might be understandable for a privacy expert, it will likely not be evident to the end user. After all, service providers collecting data on behalf of multiple controllers will have a very strong interest in presenting their platform as privacy friendly, protective, and focused on the individual in order to achieve a high turnout for their end customer, the controller. In that sense, the image given on the outside to the data subject might, at first glance, be the exact same for both types of services but in fact, leave the individual with very different actions of recourse.

The same problem also applies in the context of controllership over the transfer of datasets and consent signals. As outlined under Part 2 Chapter 4: C. II. 1. b) Collection and Transmission, the PIMS will take the role of a controller regarding both of these processing activities. The function of the end recipient will, however, again vary based on the relationship between the two entities, leading to either a separate, single controllership on the side of the PIMS where the platform is selected without any involvement of the recipient, or to joint controllership where controllers have to sign up with the PIMS in order to receive data or consent from the individual. This difference, however, only concerns the internal functioning of the platform and will again not necessarily be evident to the affected individual. While platforms might be able to explain these differences to the data subject and would have to make the essence of the arrangement with the other controllers available to such based on Art. 26(2), the distinction would not be evident when simply using the platform. Varying tools, based on various technical set-ups and fluctuating degrees of cooperation between the parties will therefore potentially look exactly the same to the end user, while at the same time having a completely different legal impact as to the ways in which compensation can be obtained. This can lead to a number of practical difficulties and arguably hinders individuals in truly taking control over their personal information. For this reason, a Personal Information

Management System should be obliged to place a high emphasis on transparently communicating not only the division of the responsive roles and responsibilities but most importantly the consequences of such for the users of the platform.

3. Relevance

At a first glance, it may seem as though the described differentiations are not in fact that significant. After all, under both scenarios, both the PIMS and the recipient would be controllers, just not necessarily in a joint capacity. It might therefore be useful to consider a practical example in order to illustrate the consequence of this differentiation and thereby underline why transparency is so crucial in this context.

In the following analysed scenario, we will designate the involved parties as the data subject (DS), the Personal Information Management System (PIMS), and a marketing company (M) wishing to process the DS's personal data for the purpose of online advertising. The DS uses the PIMS for consent management services and sets up preferences as to what type of data may be processed for which purposes. The individual regularly receives updates, and can black- and whitelist certain providers or define special parameters for some of them. The DS has filled out a consent form in the PIMS for a number of service provider' including M. For M, consent was given to process datasets A and B for marketing purposes, whereas some other providers were also allowed to access dataset C, which contains sensitive personal data. At some point, the DS finds out that M has in fact used all the datasets—A, B, and C. This has led to significant loss in reputation and confidentiality for the DS, who now wishes to claim immaterial damages in accordance with Art. 82.

a) Separate Controllers

The question occurs from whom such damages could be claimed, starting with the assumption that the PIMS and M are not in any relationship, contractual or otherwise, making them separate controllers for their respective processing activities. Art. 82(2) provides that any *"controller involved in processing shall be liable for the damage*

caused by processing which infringes this Regulation". The processing of the dataset C infringes the Regulation because no consent has been provided for such, meaning that M has no legal basis for the processing in accordance with Art. 6. The DS could therefore attempt to claim damages from M. If M processed the additional dataset, fully aware that no consent was provided, the DS would likely be successful. If, on the other hand, M was provided with an incorrect consent signal by the PIMS which indicated consent for datasets A, B and C, M could be exempt from liability based on Art. 82(3) as they would be in no way responsible for the infringement since there was a well-founded belief that they did have a valid legal basis for processing. In this scenario, the DS would therefore have to neglect their claim against M and refocus it against the PIMS who was responsible for sending the faulty consent signal. However, should the DS first make a claim against the PIMS, they might end up with the opposite outcome, namely the PIMS claiming no responsibility for the event giving rise to damages based on that fact that the consent signal, for which they are the controller, was processed correctly, thereby exempting them from liability and leaving open the option to pursue a claim against M. In consequence, an individual wishing to make a successful claim in such a case would essentially first need to investigate the reasons for which the infringement of the Regulation occurred as otherwise they might end up in multiple proceedings, with multiple parties, in multiple jurisdictions, all pointing their finger at each other and arguing a lack of liability.

b) Joint Controllers

The same problem would not occur if the PIMS and M were to be considered as joint controllers based on either an explicit contract or, for example, the requirement for M to sign-up for the PIMS platform as well. Article 26(3), after all, provides that the rights of the data subject, including the right to claim compensation, can be exercised against each controller regardless of the terms of their agreement and the division of responsibilities laid down therein. Taking this into account, the data subject will be able to claim the entirety of their

damages from either of the involved controllers based on Art. 82(4), which introduces a regime of joint and several liability. In this scenario, the argument as to the side on which the infringement which gave rise to the damages occurred, is largely left for the PIMS and M to sort out between each other. Both parties would be fully liable externally towards the DS, regardless of the specific culpability with regards to the incident that occurred, while afterwards being able to claim compensation from their contractual counterpart corresponding to their part of responsibility, based on Art 82(5).

This example very effectively demonstrates the purpose of the legal figure of joint controllership, which explicitly aims at avoiding situations in which the data subject needs to investigate the details of a specific processing activity, reasons for infringements, and the extent of culpability of various involved parties. It also clearly evidences that the seemingly small shift in roles taken by the relevant parties, which is likely completely invisible to the average data subject, leads to significant practical implications, thereby underlining the importance of transparently communicating these.

IV. Interim Conlusions: Consent

The above considerations clearly evidence not only the relevance of correctly assigning the roles of the respective parties under the GDPR but the practical implications of such a designation as well. From the basic legal analysis of the different forms in which consent management could be functioning, it should be assumed that the Personal Information Management System will take no roles with regard to the intended end processing activity for which the consent is provided. The PIMS should, however, be considered a controller concerning any transfers of personal data performed by them on behalf of the data subject, as well as the transfer of the consent signal to the recipient. The responsibility for these two processing activities might be shared with the receiving entity in the form of joint controllership, where the end controller has a contractual or other relationship with the PIMS or signs-up to the platform as well. This assumption is based on the fact that the entity interested in processing personal data will, in those cases, have selected a platform to cooperate

with, thereby essentially enabling their processing of personal data and exercising a *decisive influence on such.*

This position, however, does not seem to be shared by current platform offerings within the field. While some do see themselves as controllers with regards to certain functionalities, many very clearly exclude any responsibility under the GDPR. Their lack of responsibility under the GDPR will often be based on existing "zero-knowledge" or "no-access" policies. This argumentation, however, cannot be followed since this is not a necessary element of the designation as controller under Art. 4 No. 7 GDPR which focuses on authority over the processing activity, rather than actual performance. Another relevant element supporting the necessity of the PIMS to take the roles of a controller under the GDPR is the consideration of their relationship with the data subject in conjunction with the principle of fairness enshrined in Art. 5(1)(a). Since in many instances they would essentially primarily be interacting with the Personal Information Management System, it can be assumed that there will be a reasonable expectation of a certain level of authority, as well as responsibility for the platform services.

It should also be noted that the privacy policies of many of the reviewed providers tend to use quite vague wording, referring to elements such as "control" and "responsibility" but clearly avoiding the use of an official legal designation under the GDPR. This is particularly worrisome considering the already present issues with transparently presenting the respective obligations of the parties. Furthermore, it essentially violates the requirements outlined in Art. 12(1) GDPR to use clear and plain language while providing information to the data subject and to do so in a concise, transparent, intelligible and easily accessible form. Since their legal designation will often depend on elements such as the relationship between the PIMS and the data recipient, which is not necessarily visible to the end user, the clear and open designation of functions is even more crucial. In that sense, Personal Information Management Systems should be subject to particular scrutiny with regards to the proper assurance of

transparency and the communication modalities, as outlined in Art. 5(1)(a) and 12 GDPR.

D. Data Subject Request

The category of data subject requests, as evidenced in the first part of this thesis under Part 1 Chapter 4: D. Requests, is quite wide and involves the assurance of a multitude of data subject rights, namely those of: access (Art. 15); rectification (Art. 16); erasure (Art. 17); restriction of processing (Art. 18); portability (Art. 20); and to object (Art. 21). These differ from the previously discussed obligations of assuring secure storage, transparency, and valid consent in the sense that they generally do not require the controller to take action automatically but are rather based on the inquiries made by the data subject. While there are a number of elements specifically with regards to the form in which they are to be answered, the timing and costs of such, the possible exemptions and most importantly, the identification of the data subject, which all of these have in common, each right also has a specific character and purpose requiring exclusive attention. Analogously to the previously applied division of universal and specific considerations, the analysis of the roles and responsibilities taken by the relevant parties with regard to functionalities assuring these data subjects' rights, should therefore also be divided into two categories.

I. Universal Considerations

Whereas each data subject right has its unique purposes, rules of applicability, and forms in which they are facilitated, there are a number of rules applicable to all the rights outlined in Articles 15–22, which in a sense constitute a general framework for the handling of data subject requests.

1. General Compliance

Art. 12(2) creates a requirement for controllers to facilitate the exercise of the rights under Articles 15–22 of the GDPR, which in a sense supports the possible involvement of a Personal Information

Management System. Directly linked to this is the demand of Art. 12(5) that all actions and communications taken in order to comply with a request of a data subject should be free of charge. While a controller might be exempt from complying with a request or alternatively charge a fee, this will only be the case where such is deemed to be manifestly unfounded or excessive. Any information or action taken based on a request should be provided without undue delay and in any event, at the latest within one month after the request has been received, in accordance with Art. 12(3). In line with the principle of transparency and corresponding to the transparency requirements of Art. 13 and 14, Art. 12(1) also establishes that any communication concerning the individual's request relating to processing of their data subject, should be provided *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child"*.

All of these rules will be quite relevant for the provider of a Personal Information Management System through which such a data subject request is being transmitted. Part 1 Chapter 2: D. II. Universal Considerations outlined in much detail how explicitly a PIMS could support the individual in enforcing their rights, in the context of all of these aspects, as well as the potentially involved risks. Particularly when it comes to these rather formal requirements for handling a data subject's request, the main function of the tool would lie in monitoring the controller's compliance with the set-out framework and information for the data subject of any possible violations. This could, for example, be done in analysing the provided answers with regards to their content, as well as ease of understanding. Also, quite straightforward to implement would be a timer monitoring the controller's compliance with the legal deadline. These functionalities, while for now rarely applied within actual Personal Information Management Systems designed to be used by the data subject, are in fact

reasonably popular in the context of compliance tools designed for business users for the monitoring of their incoming requests.[143]

a) Processing of Personal Data

The determination of the relevant processing operation is relatively easy in this context. The tool analyses the content of a request, the type of right which the individual wishes to invoke and the end result which they want to achieve, as well as any additional information contained in the request. The deadline for compliance with the request is then calculated and the provided answer is monitored and documented. All of this information relates to an identified or identifiable natural person as it concerns an individualised request and not a general question or concern and is therefore to be qualified as personal data, meaning that the entire record of the handling of the request constitutes processing of personal data.

b) Determination of Means and Purposes

The question relevant for the purposes of this thesis is who is determining the means and purposes of such an operation. It has been established in Part 1 that, at the time of writing, there were in fact no fully developed service offerings which would take over the entire process of handling all types of data subject requests on behalf of an individual which could be used as a good exemplification of the current practices.[144] In that sense, while compliance tools offered to

---

[143]See for example: Data Grail, https://www.datagrail.io/platform/request-manager/ (accessed: 24 October 2025); Clarip, https://www.clarip.com/data-privacy/dsar-portal/ (accessed: 24 October 2025); OneTrust, https://www.onetrust.de/loesungen/einwilligungs-und-praeferenzmangement/ (accessed: 24 October 2025); MineOS, https://business.saymine.com/privacy-request-management (accessed: 24 October 2025); DataGuard, https://www.dataguard.de/blog/die-betroffenenanfrage (accessed: 24 October 2025).

[144]While there are service providers which specialise in the assurance of specific data subject rights or parts of them, these will be discussed in more detail in

business end users have been excluded from the definition of PIMS, taking into account that the functionalities of a PIMS would essentially mirror their service offering, it still makes sense to take a look at the division of responsibilities applicable to such, in order to gain a general understanding of the underlying problem.

aa) Compliance Tools

In the context of the multiple compliance tools offered to business users, this is quite clear. A controller processing the personal data of their customers, website users, employees, or otherwise will typically deploy such a solution in order to document their compliance with the requirements of the GDPR in accordance with the principle of accountability, enshrined in Art. 6(2). Here, the entity deciding to adopt a specific tool or software for this purpose is already the controller for the personal data, being the subject of the request. The tool is only used in order to evidence how their legal obligations towards the data subject are being handled. In that sense, the business user is both the controller for the underlying dataset, as well as the entire documentation related to the management of the data subject request. The provider of the compliance tool on the other hand might either be a processor if, for example, they are involved in the establishment of the means of processing to a certain extent or where the solution is deployed within their infrastructure on behalf of the controller. Where on the other hand, such a service provider is only delivering a software solution, installed and operated entirely by the business end user, they will be considered a third party and bear no responsibility under the GDPR.

bb) Personal Information Management Systems

The same logic can, however, not be transferred to actual Personal Information Management Systems, analysed in the context of

---

the context of each individual rights under Part 2 Chapter 4: D. II. Specific Considerations.

this thesis. Here, a tool selected by the data subject will forward and handle the individual's request on their behalf and not on behalf of the controller of the relevant dataset. In that sense, in order to be qualified as a processor (assuming that the monitoring of the request which constitutes a part of the service offering is conducted within their infrastructure), a different controller would need to be identified. Since a PIMS is, as per definition, acting in the interest and in line with the preferences of the data subject, aiming at empowering them to execute their legal rights, this would make them the processor of the individual customer. The same problem has already been discussed in the context of storage (see Part 2 Chapter 4: A. II. 2. Type of Customer) and the general idea of applying the role of "data controller" to the data subject (see Part 2 Chapter 1: A. I. 2. b) Data Subject). As has, however, already been established in therein, such an outcome should be categorically rejected, as it would essentially contradict the primary purpose of the Regulation, including the aim of assuring *"effective and complete"* protection.[145]

Whether the PIMS could, however, be considered as a processor of the entity to which the request is submitted is highly questionable. After all, not only has the platform not been selected by them, but they are certainly not acting on their behalf. If anything, the tool is rather tasked with essentially auditing the compliance of the data controller with the regulation, thereby acting directly against their interests, rather than for them. Where that is the case, it needs to be assumed that the Personal Information Management System would have to take the roles of data controller, not in the sense of responsibility of answering the data subject request, but for the processing of personal data performed as a result of managing and monitoring the administration of the request by another data controller.

If, on the other hand, controllers were to sign up to the PIMS platforms as well, as is currently practiced in the context of consent management and data portability, the PIMS might in fact be considered

---

[145]Sydow/Marsch / *Raschauer*, Art. 4, para 119; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212.

a processor. Such instances are, after all, imaginable considering that controllers might benefit from their depiction as privacy friendly enterprises willing to cooperate with platforms created for the benefit of the data subject. Should PIMS become subject to certification, as is currently being considered, this would also constitute a great benefit in the sense of legal certainty and were deployed for multiple controllers at once, even lead to savings in cost in contrast to internally operated compliance solutions. This, however, again creates the strange dichotomy in which the roles taken by the Personal Information Management System towards the data subject largely depend on their relationship with another controller and not the individual itself.

2. Identification

The second universal requirement, which will be applicable in the context of all data subject requests and also likely involve a quite significant level of processing of personal data, is the element of identification. As outlined in Part 1 (see Part 1 Chapter 2: D. I. 3. Identification) there are two forms of “defects in identifiability” which are relevant in the context of data subject requests, the first of which relates to the inability of identifying a link and the second, the requesting individual. Both of these can in a sense be considered as preliminary stages of handling such requests, since questions of identification are, in principle, to be sorted out prior to taking any other actions.

a) Identification of a Link

The first defect in identifiability, described as identification of a link, refers to instances in which it is clear by whom a request is made, however, the controller is unable to locate the corresponding dataset in their systems, thereby missing a link between the data subject and

the information relating to them.[146] This can, in fact, *often* result from the adoption of privacy friendly measures such as pseudonymisation, data segregation, encryption and access restrictions, since such, while intended to assure a high level of protection, will at the same time make the localisation of information and its combination with other sets significantly more difficult.[147]

aa) Stand-Alone Feature

Where a Personal Information Management System is solely providing the functionality of managing data subject requests, considered at this point as a stand-alone feature without any additional service offering, it will not be impossible for such to remediate this defect on the side of the controller. Where personal data is being exclusively kept within the infrastructure of another business and the PIMS is only submitting a request on behalf of their individual customer, they will naturally not be able to access or otherwise locate the data in question. This means that the localisation of the relevant datasets will therefore be performed under the exclusive responsibility of the controller receiving the request, whereas the PIMS will not be taking any role in the context of the processing of personal data performed as a result of such.

bb) Combined Feature

The remediation by a PIMS is, however, imaginable when combined with other typical PIMS functionalities, mainly consent management. Where a data subject request is not just submitted to the controller with regards to an already separately ongoing processing activity, but rather relates to a processing activity facilitated by the platform, the level of involvement can potentially be significantly higher. If, for example, the user's personal data was stored within a

---

[146] Kühling/Buchner / *Bäcker*, Art. 12, para 29; Sydow/Marsch / *Greve*, Art. 12, para 23.

[147] *Veale/Binns/Ausloos*, 8 IDPLaw 2018, 105, 115-117.

Personal Information Management System as part of a secure storage solution and then further transferred to another controller as part of the offered consent management, it would be possible for the provider to mark such datasets with additional attributes in order to enable their later discovery. This could even be combined with specific protective technical and organisational measures such as encryption, with personal data only being routed in a pseudonymised form to the end recipient but marked with a specific key allowing it localisation by the PIMS, where necessary.

Such a functionality would provide an additional layer of security to the dataset and, in that sense, further the interests of the data subject. On the other hand, the PIMS would essentially take over several obligations of the controller, namely the assurance of technical and organisational measures, the documentation of a legal basis for processing, the pseudonymisation of data, and the facilitation of localising the datasets, relevant in the context of a data subject request. This marking of the information in order to allow controllers to efficiently find it, is definitely more in the interest of the business who has to answer such a request in a timely manner than the data subject, who can be largely unconcerned about a company's internal struggles. In that sense, functionalities allowing the identification of a link, while maybe indirectly favourable to the individual whose datasets might otherwise be untraceable or lost, predominantly benefit the business required to answer the request.

Also, since the technical configurations for such an offering would need to be realised in advance to the data transfer, the recipient would be made aware of these enhancements and accept their roles as a controller in that regard. They would not be required to use the data localisation method implemented by the PIMS, having the options to revert to their internal procedures. Should such a controller, however, decide that they wish to make use of the provided functionality and receive assistance of the PIMS in locating a dataset, it should be concluded that the Personal Information Management System would in that capacity act as a processor of the data recipient as they would be acting "on behalf" of them.

b) Identifikation of the Data Subject

The second potential defect in identifiability refers to instances in which the controller has doubts as to whether or not the person making the request is in fact the data subject.[148] This is of particular relevance in the context of Personal Information Management Systems as it would be reasonable for a controller to have some doubts and wish to perform their due diligence where a data subject request is submitted through an intermediary. Assuring the identity of the individual is in fact crucial since any type of action performed on a dataset (such as, for example, submitting details of the processing activities, erasing information, or providing copies of personal data) not based on the data subject's will would essentially constitute a breach in the meaning of Art. 4 Nr. 12 GDPR.

aa) Cooperating Platforms

Questions of trust and assuring identification should not be as prevalent where the controller also signs-up as a "user" of the PIMS, such as is the case with many consent or data portability platforms. Here, the data controller would have essentially already verified the selected provider for compliance with the General Data Protection Regulation as part of standard due diligence and vendor vetting procedures. In that sense, any sort of rejection of data subject requests based on doubts regarding the platform's procedures would obviously not be admissible.

In the same vein, as with the previously discussed identification of a link between the data subject and a specific dataset, the accurate identification of the individual behind a request also essentially falls under the legal obligations of the data controller. Where therefore a controller has decided to cooperate with or sign-up to a platform, managing such requests as part of their service offering even if the data subjects are registered to such independently, the PIMS should be assumed as acting on behalf of such a controller in that regard as

---

[148]Kühling/Buchner / *Bäcker*, Art. 12, para 30; Sydow/Marsch / *Greve*, Art. 12, para 30.

they are taking over their tasks. This is particularly interesting in the context of platforms which consider secure identification as part of their service offering. The idea behind that would essentially be that the data subject simply needs to validate their identity with the platform once but can afterwards submit requests to multiple providers. The PIMS would here in a sense, provide a guarantee for the validity of the request.

The provision of such a guarantee does require a significant level of processing of personal data on the side of the platform. They are likely to have multiple verification procedures in place and will have to collect data containing some sort of proof of identity. The PIMS will also largely be determining the means of such processing independently from other actors, which might be qualified as “essential”, suggesting a role as controller. As already mentioned, the end result, on the other hand, would not only directly benefit the other controller to whom a DSR is submitted but basically take over their legal obligation. Taking this determination into account, it seems legally impossible for the business to “transfer” their controllership onto the PIMS. Whereas the means of processing personal data, in the sense of selecting how to secure the identification of a data subject, will largely be performed by the PIMS, the purpose of processing—which is far more relevant for the determination of controllership—will always lie on the side of the entity to which the request is submitted, as it is their legal responsibility. Any sort of processing required for handling a data subject request would, therefore, essentially fall under the category of “controllership based on implicit legal designation”,[149] since the General Data Protection Regulation clearly outlines the responsibilities for such.

Furthermore, since the business user will have signed up to the platform and presumably done their due diligence in that regard, it can rather be assumed that they are outsourcing the element of se-

---

[149]See Part 2 Chapter 3: A. II. 1. a) bb) Implicit Legal Responsibility.

cure identification as well. After all, the entity in question would certainly have the option to reject the PIMS guarantee of identification, where there are, for example, doubts as to the conducted review and reverse to their internal procedures. The registration for such a platform, combined with the acceptance of their guarantees on the side of the controller, can therefore be qualified as an outsourcing to the Personal Information Management System, who will take on the role of processor in the meaning of Art. 4 No. 8, with regards to the secure identifications of the data subject.

bb) Independent Platforms

Where the platform facilitating the submission of data subject requests on behalf of the individual is completely independent from the data controller, the identification of the data subject can constitute a significant dilemma. On the one hand, the controller has an obligation to verify the identity of the individual making a request, in order to avoid any risks for the rights and freedoms of the data subject.[150] Where a request is being submitted though a channel of communication not previously used between the controller and the data subject, through a platform neither known nor verified in advance, the controller might be reluctant to accept such a request, including any guarantees of identification provided by the PIMS. On the other hand, the requirement to facilitate the exercise of data subjects' rights based on Art. 12(2) in a sense forces the controller to accept the channel of communication selected by the data subject, as the refusal to do so without any serious grounds could be interpreted as the creation of an obstacle or demand, hindering the individual from exercising their rights.[151]

---

[150] *Dix* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 12 DSGVO, para 37, notes that the rights of the controller outlined in Article 12 (6) can convert into a legal obligation to confirm the identity, where serious doubts regarding such emerge.

[151] Kuner and others / *Polčák*, Art. 12, 398, 410; Eßer/Kramer/von Lewinski / *Eßer*, Art. 12 DSGVO, para 20; Sydow/Marsch / *Greve*, Art. 12, para 22.

At a first glance, the roles taken vis-a-vis the data subject would therefore need to be divided differently than in the case of the previously discussed cooperating platforms. Here, after all, the classification of the entity receiving a request as the controller and the PIMS as a processor was based on the selection of platform made by the business user, independently of the data subject. This, however, cannot be assumed here as the controller is essentially "forced into" cooperating with the Personal Information Management System. While the qualification of the PIMS in the context of identity management and verification thereby seems counter-intuitive, it should not be principally rejected.

(1) Independent Platforms as Processors

When taking a closer look, it is clear that the service provided by the Personal Information Management System would essentially be the same, both in the context of cooperation, as well as independent platforms. The only relevant difference constitutes the lack of selection on the side of the controller. This notion, however, is not entirely true. The controller is able to reject the submission via a specific PIMS if there are reasonable grounds to do so. The controller would also certainly have the option to answer the request via the platform, based on the requirement of facilitation but not to acknowledge the identification procedure performed by the PIMS, insisting on their own standards, due to security concerns. Also, while they cannot select the use of a different PIMS provider altogether, this selection is also only limited in the context of cooperating platforms, as here the management of the data subject request would also only be possible via the Personal Information Management System with which the data subject has registered, excluding any other providers.

In that sense, data controllers are not deprived of their option to choose but are simply left with a "take it or leave it" approach, whereby they could use the identification service of the PIMS or deal with the consequences of rejecting such. Scenarios of limited or in a sense illusive choice are, however, nothing new in the market realities and are not exclusive to PIMS. As has been outlined both in the context of the role of processor (see Part 2 Chapter 3: B. II. 2. On

behalf of the Controller) and with regards to the qualification of cloud storage (see Part 2 Chapter 2: A. II. 1. Types of Clouds), imbalances of power between the actors are in fact not uncommon and processors are not precluded from being the stronger counterpart. While the GDPR in principle construed the relationship between controllers and processors as one of subservience where the latter should be acting in accordance with the instructions of the first, it is commonly known that these are not necessarily the practical realities, and processors actually quite often pre-dictate the form in which they are to handle personal data, should their services be used.[152] The EDPB also explicitly confirms in that regard that processors are not precluded from offering preliminary defined services and that the essential determination made by the controller lies in selecting this specific service offering.[153]

(2) Independent Platforms as Joint Controllers

When a controller does not select the Personal Information Management System personally, in the case of independent platforms, this should not per definition exclude them from being considered data processors; rather, the overall circumstances, including the possibility of them rejecting identification through the PIMS, need to be accounted for.

Where a controller has reasonable grounds for rejection depending on the identification procedure performed by the PIMS, this does not release them from the obligation to act on the request. Rather, they will need to revert to their existing identification procedures or

---

[152]See for example the standardized: AWS Service Level Agreements, https://aws.amazon.com/legal/service-level-agreements/?aws-sla-cards.sort-by=item.additionalFields.serviceNameLower&aws-sla-cards.sort-order=asc&awsf.tech-category-filter=*all (accessed 25 October 2025); IBM Cloud Service Level Agreements, https://cloud.ibm.com/docs/overview?topic=overview-slas (accessed 25 October 2025); Google Cloud Platform Service Level Agreements, https://cloud.google.com/terms/sla (accessed 25 October 2025); Microsoft Azure Service Level Agreements, https://azure.microsoft.com/en-us/support/legal/sla/ (accessed 25 October 2025).

[153]*EDPB*, Guidelines 07/2020, para 82.

consider other alternatives. Since the data subject has decided to submit their request via the PIMS and not personally, the controller will also need to, as far as possible, respect that wish in accordance with the requirement of facilitation and make a serious attempt to communicate with the platform provider. The controller will need to communicate their doubts and identified gaps, as well as provide suggestions as to a possible resolution. The PIMS could then either attempt identification through the existing procedures of the controller using the available data or come up with alternative solutions. They might also provide the controller with additional input into the functioning of the platform or their privacy policies in order to resolve any existing uncertainties on the side of the controller, which would lead to a delay in answering a request. Either way, doubts on the side of the controller as to the safety or validity of the platform will lead to a form of communication and cooperation between the two parties, who will need to decide on the further steps in which the data subject request is to be handled.

In that case, both parties will have an inherent interest in resolving the issue and acting in accordance with the data subject request. The Personal Information Management System will do so based on their service relationship with the data subject and the controller based on their legal obligation. In that sense, the parties will have a joint purpose in establishing a valid form of identification for the data subject. Each party also has their own legal basis for any processing of personal data necessary to pursue that aim, for example, Art. 6(1)(b), the contract with the individual and the controller receiving a request, and Art. 6(1)(c), compliance with a legal obligation which arises directly from the GDPR. As laid down in the previous paragraph, they will also co-operatively establish the exact means by which this goal should be achieved. Thereby, they will jointly determine the means and purposes of the processing of personal data required for the valid identification of the data subject. This, as per definition, very clearly makes them joint controllers in the context of this specific processing activity.

3. Interim Conclusions: Universal Considerations

The GDPR provides for a number of requirements which apply in the context of assuring all of the data subject rights outlined in Articles 15-22. Broadly speaking, these concern on the one hand formalities such as format, time and content, and on the other, the question of identifiability.

PIMS are able to support these modalities relating to the formalities in multiple ways such as, for example, analysing the provided answers for comprehensibility and completeness or monitoring the adherence to deadlines. While similar functionalities are already present in standardised compliance tools which will typically act as processors on behalf of the controller to which the request is being submitted, this legal designation cannot be easily transferred onto PIMS due to their differing purpose of processing. Since Personal Information Management Systems will in principle process personal data against the controllers' interest and in accordance with the data subjects' preferences, it should be assumed that they will take the role of a separate data controller in their own right for the processing operations being performed as a result of managing and monitoring the administration of the request by another data controller. This assumption will, however, not necessarily hold true where data controllers are also signing up as customers of the PIMS platform which can, for example, be observed in some tools offering consent management and data portability services. Here, the PIMS might take the role of a processor, since the management of the request will be performed on behalf of the controller in that context.

The two possible defects in identifiability can relate to the identification of a link between a dataset and the data subject, and to safeguarding the identity of the individual making the request. Where a PIMS does not offer any functionalities in addition to the submission of requests, it is unlikely that the tool would be able to support the establishment of a link in any significant way. If, on the other hand, it was to be combined with modalities such as consent management or secure storage, the service provider might be able to ensure the identification of relevant datasets. Considering that the PIMS would, however, essentially take over a task a controller is legally obliged to

perform, thereby acting in their interest as well as those of the individual, they should be qualified as processors for such functionalities.

In the context of safeguarding the actual identity of the individual making the requests, the legal classification of the platform will mainly depend on the relationship between the controller and the PIMS and not on the technical parameters of identification. In the case of so-called “cooperating platforms” where the controller has also registered as a user of the PIMS, the tool will act as a processor on their behalf, taking over their legal obligations. Arguably, the same role would be taken where a request is submitted through an independent platform with which the controller is not formally cooperating but still agrees to the identification procedure suggested by the PIMS, in that sense accepting their offer. Where on the other hand, a controller decides to reject the PIMS’ means of identification based on a lack of trust or concerns regarding the implemented technical and organisational measures, they will in a sense be forced to agree upon alternative means with the provider, making them joint controllers. This leads to a paradox by which the legal designation of the PIMS will be dependent on the controller’s acceptance of their identification procedure.

II. Specific Considerations

Whereas all the data subject rights outlined in Articles 15–21 of the GDPR have certain elements concerning the formal and procedural requirements of their management in common, the underlying purpose and consequences of each are completely different. In the same vein, the functionalities offered by the Personal Information Management System, in order to facilitate the exercise of those, are also incredibly diverse. Both the existing tools, as well as considerations for further developments and improvements, have been presented in Part 1 Chapter 2: D. II. Specific Considerations. The subsequent section will therefore analyse the roles and responsibilities taken by the PIMS and the entity receiving a request towards the

data subject in the context of each of these specific rights and the connected service offerings.

1. Access

As has been previously established, the right to access essentially contains three components which may be invoked together or separately, depending on the circumstances. These are the right to obtain: a) confirmation; b) details about the processing; and c) a copy of the data; as well as arguably in some instances, d) only access.

a) Confirmation

Article 15(1) of the GDPR provides that each individual has the right to obtain a *"confirmation as to whether or not personal data concerning him or her are being processed"*. This can serve multiple purposes such as assuring that a controller who should have deleted an individual's personal data by a certain date, has in fact ceased the previously carried out processing activity, or where no deletion period has been established, determining whether these activities are still ongoing. The GDPR also does not preclude individuals from submitting a so-called "precautionary request", where a data subject might not have been in any previous contact with a specific business and have no explicit basis to assume that their data is being processed by a specific entity but still would like to receive a confirmation in that regards. Such requests are particularly popular in fields such as online advertising and marketing since here data subjects might often have "consented" to the sharing of personal data with a large amount of third parties through a cookie banner, without actually being aware of it at the time. Personal Information Management Systems can aid this curiosity either through submitting requests on behalf of the individual or by conducting a form of "pre-selection" or "pre-confirmation".

aa) Pre-Confirmation

The functionality described herein as a "pre-confirmation" is part of certain tools which largely focus on the facilitation of another data

subject right, typically the right to deletion or objection, but perform a sort of automated pre-selection of controllers towards which these rights may be invoked. The tools Revoke,[154] DeleteMe,[155] or Mine[156] will, for example, as a first step perform searches on the client's mailbox, the dark web, or various databases identifying where the client's personal data is being held. Based on that, they will send out requests to the respective businesses, exercising the individual's rights on their behalf. Such an initial search can, however, be qualified as a processing activity in itself as the provider will need to collect the user's personal data and either run it though a number of external databases, or search the individual's internal sources, such as e-mail or a social media account for information on third parties which might be in possession of their data. This search is, however, conducted completely independently from any other actors who might be processing the individual's personal data for their own purposes and regardless of the achieved results. While contact between the PIMS and the identified controllers will likely be made afterwards, based on the result these will also relate to a different part of the functionality which constitutes the invocation of the respective underlying data subject right. The performed "pre-selection" of potential controllers can, however, also theoretically result in a "negative outcome" whereby no unwanted activities are identified and the user is informed that their data is not present in any of the analysed databases, which is why it needs to be considered separately from the potential subsequent actions. In that sense, the PIMS will be acting as a sole controller with regards to the processing of personal data necessary for the "pre-confirmation" functionality as they are the ones establishing both the purposes and the means by which it should be achieved, independently from any other parties.

---

[154]Revoke, http://revoke.com/ (accessed 22 February 2026).
[155]DeleteMe, http://joindeleteme.com/ (accessed 22 February 2026).
[156]Mine, http://saymine.com/ (accessed 22 February 2026).

bb) Submission for Confirmation

On the one hand, a request can naturally be submitted based on a pre-confirmation discussed in the previous point. The PIMS may also generally take over the submission of data subject requests for the data subject, regardless of such. Submissions relating to the exercise of other data subject rights such as deletion, objection, or other elements of access such as the receipt of a copy shall, however, be discussed under those respective points. What is, nonetheless, also at least imaginable are generalised submissions of requests for confirmation. A service provider might, for example, be tasked with simply generally sending out inquiries, asking whether personal data of a certain individual is being processed in order to identify where their personal data lies and reporting the results back to the data subject. These could be more or less specialised, such as, for example, asking a service provider to provide an overview of what type of advertising companies are processing an individual's information or what information can be accessed through search engines. Also imaginable would be the investigation based on a list of recipients provided by other controllers. As is commonly known, consent notices such as cookie banners frequently include long lists of potential data recipients with whom data might be shared. It is therefore imaginable that an individual might be interested in finding out to whom the data has actually been submitted. A PIMS could, for example, contact the respective parties based on such a list in order to enquire whether or not personal data of the user is being processed and for what purposes. At the end, the platform could then generate a report providing the individual with an overview of parties in possession of their data, which can either be relevant on a standalone basis or used as a decision basis for furthering the exercise of additional rights.

The creation of such overviews or reports will again require the processing of the individual's personal data, both in the form of submissions to other parties, as well as collecting the relevant answers, reviewing them and then combining and aggregating such into an understandable and suitable format. In the same vein as concluded in the context of pre-confirmation, this operation is performed by the

Personal Information Management System independently of the other potential controllers who do not have any influence over the ways in which this information is collected and how it is further analysed and presented to the individual. While they are arguably pursing at least similar purposes in the sense of providing the data subject with an overview of where their data lies, the aim of the PIMS is to overarch the individual legal obligations of each contacted controller, as the added value specifically lies in the summarisation and aggregation of the received input and not in the individual answers. In that sense, the Personal Information Management System should again be viewed as a separate controller in the context of submitting requests for confirmation on the individual's behalf. This, however, does not preclude the tool from taking the roles of a joint controller or processor with regards to other procedures, which might precede that stage or appear subsequently, such as the identification of the individual, the monitoring of deadlines, or submission of objections.

b) Details

In accordance with Art. 15(1), where a controller has confirmed that they are processing personal data of an individual or where that individual is already aware of ongoing processing activities, the data subject has the right to receive detailed information regarding such. The type of information which should be provided largely mirrors the elements already required in the privacy notice, in accordance with Articles 13 and 14, but should also relate to the specific processing conducted on the personal data of the person submitting the request and not just processing conducted by the controller in general.[157]

---

[157] *EDPB*, Guidelines 01/2022, para 20; Kuner and others / *Zanfir-Fortuna*, Art. 14, 434, 462.

aa) Existing Service Offerings

As has been explored in Part 1 Chapter 2: D. II. 1. b) dd) Existing Initiative: Access My Info, the amount of initiatives and tools attempting to support individuals in their right to access is at the moment surprisingly low, especially taking into account the practical relevance of this specific legal basis. The reviewed "Access My Info" initiative, which assists individuals with the generation of a customised access request, was as of the time of writing only able to create such activities for Canada and Hong Kong[158] and did not even submit those on behalf of the data subject, but instead asked the user to do so personally.[159] Both the amount of personal data being processed by the provider, as well as their involvement in the overall facilitation of the data subject right, is therefore remarkably low. Whether or not they would even fall under the definition of a Personal Information Management System is, in that sense, at least debatable. Regardless, however, it can be concluded that for the limited extent to which they might process the users' personal data while generating the text of such a request, they will be considered as controllers. Such controllership does not, however, go beyond any processing conducted by any other online tool producing other types of letters such as terminations, resignations, thank-you notes, or resumes. It is also clearly separate from the recipient of such a request, as all communication is still handled personally by the data subject and the provider does not intervene with such in any way.

bb) Potential Advancements

While currently existing initiatives do not offer an extensive amount of room for discussion, when it comes to the roles and responsibilities taken by such tools, the chapter concerning the provision of details about the processing of personal data in the context

---

[158]Access My Info Citizen Lab, https://accessmyinfo.org/ (accessed: 29 March 2026).

[159]*Hilts/Parsons*, PETS 2015, 1, 2.

of access rights did also provide some suggestions for possible future advancements within the field, which should also be considered.[160] Most importantly, existing machine learning and natural language processing methods, already applied in the context of transparency enhancing tools, might be used in order to audit the content and accuracy of the answer provided by the controller. Since data subjects generally report that better quality results are received after following up with the controller,[161] an automated review of the provided answer, either based on the type of information submitted, its phrasing, or accuracy, could constitute a significant advancement.

On the one hand, a reference to the functionalities analysed in the context of transparency enhancing technologies might be contemplated. There is, however, a significant difference between the analysis of a privacy policy or notice and the answer to a data subject request which might make such a comparison unsuitable. Both interpretative and auditing tools have been divided into such, providing personalised and standardised input. In the context of interpretative tools, the difference lies in either giving the data subject a standard review or translation of the policy, whereas a personalised translation would focus on elements explicitly identified by the data subject as important to them, leading to the PIMS itself processing personal data in order to provide the offered functionality. In the same vein, audits of legality or accuracy of the information could either be performed in a general manner or based on the specific processing, applicable to the end user. This division, however, cannot be applied in the context of data subject requests. As has been explored in Part 1 Chapter 2: D. II. 1. b) aa) Relationship with the Right to Information, the answer provided by the controller as a result of a data subject request should directly relate to the specific processing of personal data concerning the data subject submitting the request, whereas generalised answers or simple reference to existing privacy policies

---

[160]See Part 1 Chapter 2: D. II. 1. b) dd) Perspectives for Advancement.

[161]*Mahieu/Asghari/van Eeten*, 7 IPR 2018, 1, 12; *Ausloos/Dewitte*, 8 IDPL 2018, 4, 15.

are in principle not sufficient. If the provided answer relates directly to the processing concerning an identified or identifiable individual, it will also fall under the definition of personal data in accordance with Art. 4 No. 1. Consequently, any automated review conducted by the PIMS on the provided information will also need to be considered as processing of personal data, regardless of whether or not the functionality is subject to any additional personalisation.

Since the PIMS, offering an automated audit or "pre-review" of the details submitted by the data controller, will be processing personal data, the question occurs in which capacity this is done. In the case of compliance tools providing the same functionality, they would be typically considered a processor since they are doing so on behalf of the controller, supporting them in the fulfilment of their legal obligations. In this case they are, however, not really acting in the interest of the controller but rather against such, possibly identifying a wrongdoing on their part. The PIMS will definitely be acting in its own capacity, determining how the submitted answers are reviewed, what kind of issues would be flagged, and what the consequences could be. In that sense, they will be considered a controller as they are determining both the means and purposes of the processing activity. It also will generally not be impossible for the controller providing the answer to have any sort of significant impact on the analysis, since this would essentially defeat its entire purpose. In that sense, there is no element of cooperation or joint determination between the parties, rendering the PIMS as the sole and separate controller for the processing of personal data involved in the reviewing the provided details.

c) Copy

As per Art. 15(3) data subjects also have the right to be provided with a copy of the personal data undergoing processing.

aa) Security of the Copy

Once data leaves the presumably safe storage space and is transferred to another repository, new security concerns pertaining to the risks involved in the transmission itself will arise. This applies to the

same extent to the transfer of a copy of personal data, as to any other information. Studies completed in the field have evidenced that the procedures established by controllers in this context are frequently lacking in the necessary security measures, both in the context of secure identification, as well as the form of transmission.[162] In that sense, it has been suggested in Part 1 that the provision of a secured transfer channel for the submission of a copy or in fact any datasets by a Personal Information Management System would therefore constitute a practical and useful addition for such offerings.

Unlike the previously discussed feature, this functionality would, however, not only benefit the data subject whose data is being protected but to a large extent also the controller from whom the data is obtained. After all, the assurance that the copy or in fact any other personal data is processed in a secure manner, including its transmission to other repositories, falls under the obligation of the controller based on the general principles of integrity and confidentiality laid down in Art. 5(1)(f), as well as Art. 32(1), which requires the implementation of technical and organisational measures ensuring an appropriate level of security. These legal obligations are also inherently connected to the controller and cannot be simply transferred onto another entity. Where therefore a PIMS would offer a secure transfer channel, the controller receiving the request would not be able to simply use such without doing their due diligence and vetting the provider accordingly. It has, after all, been established that while the preferences of the data subject regarding the form and format in which information is being submitted to them need to be taken into account by the controller, they are in the end not binding.[163] If an entity, therefore, came to the conclusion that the "secure channel" offered by the PIMS was in fact lacking in essential protection, they would not only have the option to decline its use but in fact be legally required to do so. Consequently, while the data subject is the one

---

[162] *Di Martino and others*, in: USENIX 2019, 371, 374-379; *Bufalieri and others*, IEEE 2020, 75, 75ff.

[163] Kühling/Buchner / *Bäcker*, Art. 15, para 40.

selecting to submit a request through the Personal Information Management System, the final determination as to whether or not the tool can be used for the transfer of a copy of personal data will be made by the controller. In that sense, the submission via the PIMS by the end user can merely be understood as a "suggestion" of a provider, offering a secure transfer functionality. The controller would then decide whether or not they intend to use the suggested provider to transfer a copy of personal data on their behalf. It can therefore be concluded that the Personal Information Management System would be acting as a mere processor in the context of a service offering a secure transfer channel for the submission of a copy of personal data.

bb) Request Specification

As has been explored in Part 1 in the context of the right to receive a copy,[164] the relationship between this right, the general right to access, and the right to data portability is *often* questioned, and controllers frequently face practical problems in determining the true intent of data subject requests submitted in a very generalised manner.[165] Based on this, it has been suggested that where data subject requests are submitted through a Personal Information Management System, the tool should ideally include a finely grained drop-down menu, allowing the data subject to understand what kind of options they have and at the same time, specify their intent. Such an inclusion, while easy to implement, would benefit both the individual as well as the controller tremendously, excluding any type of unnecessary processing of personal data or back-and-forth discussions prior to complying with the individual's wishes. This functionality would, however, also require the processing of personal data by the PIMS as the intent of the data subject, including any specifications regarding such, naturally relate to the individual, resulting in the collection

---

[164]See Part 1 Chapter 2: D. II. 1. c) aa) Relationship to Data Portability and (2) Relationship to other Access Modalities.

[165]Paal/Pauly / *Paal*, Art. 15 DSGVO, para 33; *Zikesch/Sörup*, 6 ZD 2019, 239, 239f.

of this information and the subsequent transmission of such to another entity, a processing activity on its own.

Whereas the specification of a request is in the interest of the controller receiving such, the functionality can, however, not be equated to the previously discussed provision of a secure transfer channel. Here, while certainly benefiting the controller, the functionality does not relate to any direct legal obligation on their side. The controller is not obliged to provide the data subject with any special features, allowing the specification of the request. As long as the exercise of the data subject rights is facilitated in general, any form of communication with the individual is deemed satisfactory. Where the individual decides to submit their request in such a specified form, the controller will also at no point have the option to decline this submission or insist upon the use of the channels established by them. The Personal Information Management System will both specify what kind of options are being offered to the data subject, their level of granularity, and how they are saved and further submitted. It is therefore clear that the PIMS will not act as a processor but rather a controller in regard to the processing of personal data related to the functionality, allowing a detailed specification of a data subject request.

Since, however, the described functionality does benefit the controller receiving such a request, possibly alleviating them from the performance of any unnecessary actions or requesting specification from the individual themselves, the presence of joint controllership might be considered. While the PIMS will predominantly be establishing what type of information is being collected and how, thereby determining the means of the processing of personal data, the parties do in a sense have a common purpose as they are working towards the effective facilitation of the individual's data subject rights. The assumption of joint controllership will nonetheless not be possible due to one significant limitation. While the entity to which a data subject request is being transmitted will likely be a data controller for processing activities concerning that individual, this is in no way certain. After all, data subjects are allowed to send enquiries where they

simply suspect that their data is being used or just want a confirmation that this is not the case. It might, therefore, be absolutely plausible that the recipient of a data subject request will not be processing any personal data of that individual and simply submit a negative answer. For such instances, the entity receiving the submission will have neither benefited from the specification, nor had any own underlying interest in such. In effect, the Personal Information Management System will, therefore, need to be considered the sole controller for the processing of personal data involved in features, allowing the specification of data subject requests prior to their submission.

d) Access Only

While Art. 15 of the GDPR does not explicitly introduce a right to "only access" personal data, it can be indirectly derived from the provision. The detailed considerations on that topic have been outlined under Part 1 Chapter 2: D. II. 1. d) Access Only. It will usually apply where the compliance with one of the other access modalities, such as the provision of details regarding the processing or a copy of the data, would prove impossible based on Art. 15(4), as it might adversely affect the rights and freedoms of others. In such instances, allowing the option to access one's information in a non-permanent form such as time-limited remote access without the option to download files, onsite inspections, or even the provision of oral information might be considered a proportionate solution in order to assure that the rights of all parties are accounted for.[166] In most instances, the application of the "access only" right will, however, exclude the involvement of a Personal Information Management System. First of all, most non-permanent access modalities such as on-site visits or remote access will need to be fully managed by the data controller. Secondly, even where the involvement of the PIMS might be technically feasible, the possible effect on the rights and freedoms of others which have been identified as relevant in that context, will require

[166] *EDPB*, Guidelines 01/2022, para 133.

that the range of the involved parties be kept to an absolute minimum, effectively excluding the PIMS from the scope as such. In that sense, a Personal Information Management System is unlikely to take any role under the GDPR where the controller has a reasonable legal basis for denying the individual with the provisions of a copy of their personal data, but rather needs to revert to only providing temporary access, based on Art. 15(4), instead.

e) Interim Conclusions: Access

For most of the reviewed functionalities, related to supporting the individuals right to access under Art. 15 GDPR, the PIMS will take the role of a independent data controller. First, searches by a PIMS on the client's mailbox, the dark web, or other databases identifying where the client's personal data is being held, conducted as a part of the "pre-confirmation" functionality, are performed independently from any other actors, who might be processing the individual's personal data for their own purposes and regardless of the achieved results. Secondly, when submitting requests for confirmation on the individual's behalf and presenting the data subject with an aggregated overview of the results, there is also no element of cooperation or joint determination between the parties. Finally, while the party receiving a more specified data subject request, as a result of a "specification" functionality, might benefit from the PIMS service, there might still be instances where the receiving entity is not processing any personal data of the PIMS user. Since therefore joint controllership would be impossible, the PIMS will again need to take the function of the sole data controller, for the submitted request. The one instance, where a PIMS is likely to take the roles of a processor, is related to the offering of secure data transfer functionalitites. Here the other data controller, in possession of the dataset, is legally required to ensure the security of the data transfer. This obligation cannot be transferred onto onther party, other than in the form of a controller-processor relationship. As a result, the PIMS will thereby be a processor under Art. 28 of the GDPR, for this specific functionality.

2. Rectification

Stemming from the principle of accuracy enshrined in Art. 5(1)(d) of the GDPR, Article 16 introduces two forms of rectification: the correction of incorrect information and the completion of incomplete personal data. For both of those modalities, the introduction of a feature allowing for personal data to be directly corrected or updated across multiple systems where a change is being made within the PIMS, would constitute a significant advantage for the data subject, who as a result will not need to inform each data controller separately. A form of automated or direct rectification could be facilitated in multiple ways, which are also likely to differ with regards to the roles and responsibilities taken by the parties and should therefore be discussed independently.

a) Rectification at the Source

Where the Personal Information Management System is also storing the user's data as part of their service offering, it is possible that the PIMS would only allow other controllers to access such as part of a consent feature, rather than actually transfer any information. This would certainly be beneficial from the point of security as it would avoid multiple copies of a dataset being scattered around multiple systems. While the information will not be within the scope of direct authority of the other controller who is only accessing the data through the PIMS systems, it still allows them to process it for the purposes for which consent has been provided. In such a set-up, any changes to the information which are being made by the data subject will therefore only need to be applied in the original dataset, without the need for any further actions.

This solution, however, cannot function independently from other functionalities such as storage and consent. Its implementation will also only be possible in the context of platforms which cooperate with the data controllers in some form or another. The controller will, after all, need to access the dataset through the PIMS, meaning that the platform and the other actors will have had contact prior to the rectification of the dataset. The parties will also need to have decided on

the specific extent and modalities of the access given to personal data, the purposes, timeline, etc. In the same vein, the inclusion of the direct rectification will also be inextricably linked to such a service offering. While the PIMS will in a sense take over the responsibilities of the controllers by accessing personal data through their system based on consent or other applicable legal bases, thereby acting on their behalf, the inclusion of such a functionality will also be done for their own purposes, namely the service relationship with the data subject. Additionally, they need to determine the essential means of the processing in that context, as they are not only holding actual physical control of the data but also doing so, regardless of the other controllers, based on their direct obligations towards the data subject. In that sense, they should not be viewed as a processor but rather as a joint controller with any other entities, processing the data subject's information and benefiting from the direct rectification feature.

Such an assumption is also generally supported by the wording in Art. 26(1), which explicitly requires joint controllers to determine their respective responsibilities *"in particular as regards the exercising of the rights of the data subject"*. If personal data is therefore kept within the infrastructure of the Personal Information Management System, it is simply logical to assume that they would be the entity responsible for the assurance of the right of rectification, as well as probably other similar rights such as erasure or restriction. The same will, after all, also typically apply for more traditional forms of joint controllership such as common databases or research projects, where the party having the actual command over the datasets is most likely to be responsible for the assurance of these rights.

b) Creation of a Link

Another option is the creation of a link between the different data stores of the PIMS and the other controller, causing direct correction of changes to certain datasets across systems once rectification has been triggered in the PIMS. This scenario differs from the previously discussed solution in the sense that there is not one dataset under

the control of the Personal Information Management System which is being accessed by other parties but that there are multiple datasets stored in the infrastructure of each of the involved parties separately. These datasets will also be processed by the respective actors for completely separate purposes and in principle without any involvement from the PIMS, other than the initial collection of consent or the transfer of the data on behalf of the data subject. They will therefore constitute separate processing activities, done by separate controllers.

The rectification itself, however, cannot be considered as truly separate, since the entire purpose of the rectification functionality is to make it dependent on the changes done within the Personal Information Management System. Therefore, the creation of a link between the datasets would essentially lead to multiple stand-alone processing activities being connected by this one feature. Taking into account the "stage-based" approach to data processing introduced by the CJEU in the case of *Fashion ID*,[167] the correction or completion of the dataset might, however, be considered as a separate element from the other underlying processing activities. It serves its own purpose: the efficient rectification of the individuals' personal data. All parties have this purpose in common and they have in advance jointly agreed upon the means by which this purpose should be achieved: namely the facilitation through a link created by the Personal Information Management System. Based on that, they would therefore also likely be considered as joint controllers.

c) Automated Notifications

Also possible, while arguably less sophisticated, would be the generation of automated notifications sent to multiple controllers where a change is being made to a set of personal data. In this scenario, there would be no connection between the various datasets. Each controller would again be processing the same personal data

---

[167]For more details refer to Part 3 Chapter 5: C. III. 3. d) ff) Fragmentation and Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

for their own, independent purposes and would determine the means of the processing entirely completely autonomously. They would control such elements as the form in which the data is stored, by whom, and when it can be accessed, as well as when and how it would be deleted. The facilitation of the right to rectification would also still lie within the responsibility of each party individually, as the notification in a sense only constitutes an indication for the receiving controller that an action should be taken, but does not trigger such in itself.

While the underlying processing activities are therefore entirely separate, the question occurs what the respective roles and responsibilities of the parties in relation to the submitted notifications might be. After all, the information that a dataset is not correct or incomplete also relates to the individuals who it concerns, rendering the notification itself personal data in the meaning of Art. No. 1. Unlike in the previously discussed solutions of rectification at the source and creation of a link, the submission of a notification does not necessarily require the existence of any prior communication or relationship between the notified data controllers and the PIMS. Therefore, cases of submitting information based on the controller's request, or independently of such, should be differentiated.

aa) Automated Notifications Requested by the Controller

One possibility implies that the controllers explicitly request a notification from the Personal Information Management System to be submitted to them where a dataset requires rectification. Such a functionality will likely make sense in the context of platforms requiring the registration of the controllers, as well as the data subject, which is regularly the case in the context of consent management. Here a party will sign-up for a PIMS in order to receive a set of personal data through the platform and might at the same time, ask to be informed should there be any relevant changes. While this functionality is also likely to be related to other service offerings such as consent management, the provision of information, or secure data transmission, this is not necessary and its existence as a stand-alone

functionality for which parties can register is absolutely technically feasible. In the same vein, the receipt of a notification might be offered as an additional service to the controller using the platform, for which they can sign up independently from any other service offerings.[168] Where the controller requests to be notified by a Personal Information Management System where datasets have been identified as incorrect or incomplete and can make such a selection freely and without any influence from other parties, the platform will essentially be acting on behalf of such a controller, as the occurrence of a specific processing operation would be left entirely up to them. For notification features set up in this format, the PIMS would therefore need to be qualified as a processor for the processing of personal data, resulting from the submission of a notification to the relevant parties.

bb) Automated Notficiations Requested by the Data Subject

The second possibility, which is definitely more centred around the preferences of the data subject and therefore arguably closer to the definition of a Personal Information Management System, would be an automated submission of notification of controllers, triggered by the data subject itself. In the context of cooperating platforms requiring the registration of the controller, the difference would lie in the fact that the data subject would select whether or not to activate the notification feature and not the data recipient. Notifications could, however, also be triggered by individuals in the context of independent platforms, for example: (1) through the initial provision of a list of all parties, which should be informed in the case of changes to a dataset, submitted by the data subject upon signing up to a platform;

---

[168]For example, an entity might sign up for the platform in order to use their consent management feature and while using such, be asked whether or not they also wish to receive a notification in case any changes are made to the dataset. It would, however, be open for them to decide whether or not they are interested in this feature or simply wish to keep using the "basic version" of the selected functionality.

(2) by means of scanning the data subjects' sources, in order to identify possibly affected controllers; or (3) in the form of tracking by the platform to whom data is being submitted and thereby automatically generating a list of entities.

Either way, such notifications would, however, be submitted independently of any preferences communicated by the informed parties, excluding the assumption that the PIMS would be acting "on behalf of" such. The Personal Information Management System would rather be acting based on the instructions given by the data subject, in order to provide the offered service. In that sense, they should be rendered a controller for the processing of personal data involved in the submission of notifications to other parties. Such controllership would also be separate from that of the other involved entities, since there would be no element of cooperation between them.

d) Interim Conclusions: Rectification

The example of including a functionality supporting data subjects in the exercise of their right to rectification again quite accurately demonstrates how the various technical implementations of essentially the same service offering, have a significant impact on the roles and responsibilities of the involved parties. Both in the context of direct rectification at the source and the creation of a link between datasets, the PIMS and the controller, processing the individual's personal data for their own purposes, have been rendered as joint controllers. Changes in the technical means of application for the assurance of this right will, however, cause a meaningful shift. Where there is no actual link between the datasets and a controller is only notified that a change is necessary by the PIMS, the platform will no longer be qualified as a controller but merely as a processor, thereby seriously limiting their legal obligations, as well as level of liability towards the data subject. This shift is the more crucial, taking into account that the average user, simply signing up for a PIMS platform, might not even be aware of how exactly their rights are being invoked, arguably making the existence of such a shift invisible to most individuals. Further aggravating this issue is the fact that the PIMS

will take a third role, namely that of an independent controller, where automated notifications are triggered by the data subject but no link between the datasets exists. Here the liability of the other controllers for the processing of personal data, necessary for the submission of a notification is excluded, again arguably without the knowledge of the affected individual, who might not be aware of the technical details of a rectification functionality.

3. Erasure

As has been established under Part 1 Chapter 2: D. II. 3. Erasure, this right, given to individuals in Art. 17 of the GDPR, lies at the heart of the idea of informational self-determination which is directly linked to the concept of human dignity and serves the objectives of not one, but multiple principles of data protection: purpose limitation, data minimisation, storage limitation and in a sense, integrity and confidentiality, as well.[169] It is, however, not to be understood as an absolute right since the General Data Protection Regulation provides both for very specific instances under which it should apply (Art. 17(1)) and when its exercise should be excluded (Art. 17(3)). Based on its practical relevance, the complicated legal grounds for its applicability, as well as the technical difficulties occurring in the context of its assurance, multiple forms of supporting this right have been contemplated in Part of this thesis. The specifics for each considered “improvement” will therefore be analysed in the subsequent text.

a) Request Submission

While the right to erasure is typically grouped within the category of “data subjects requests”, it also contains instances of automatic applicability, namely where the personal data is no longer necessary

---

[169] *RouvroyPoullet*, in: Reinventing Data Protection?, 45, 58-61; *Lynskey*, The Foundations, 94-99; *Frosio*, 5 Colo. Tech. LJ 2016, 307, 313ff; Schwartmann/Jaspers/Thüsing/Kugelmann / *Leutheusser-Schnarrenberger,* 'Art. 17' DSGVO, para 6.

for the purpose for which it was processed (Art. 17(1)(a)), where it has been processed unlawful (Art. 17(1)(d)), and where it needs to be erased for compliance with a legal obligation (Art. 17(1)(e)). In that sense, any "requests" for erasure based on those grounds are rather to be qualified as notifications or reminders. Requiring a form of action from the data subject are, however, the legal bases found under Art. 17(1)(b), (c) and (f), which refer to the option to object to a processing operation, as well as withdraw consents in general and specifically such given by children in relation to information society services.

Regardless of the specific legal basis, the service offering of PIMS will likely relate to the submission of requests, whether or not those are to be qualified as a reminder or an assurance that an already applicable obligation is being complied with, or whether the platforms would actually initiate the exercise of the rights. The submission of the demand of the data subject to multiple controllers has already largely been discussed in the context of the right to access (Part 2 Chapter 4: D. II. 1. a) bb) Submission for Confirmation) and the right to rectification (Part 2 Chapter 4: D. II. 2. c) bb) Automated Notifications Triggered by the Data Subject). For both of these, it has been concluded that the individual's intentions fall under the definition of personal data in accordance with Art. 4 No. 1 and the transfer of such to other parties therefore constitutes a processing activity. It has also been established that since such submissions are being made solely based on the decision of the data subject, regardless of the recipients, the Personal Information Management System is to be qualified as the sole and independent data controller for the related processing. The same will also apply to any sort of progress reports or statistics regarding the state of the requests, their success rate, or level of compliance provided to the individual user.

b) Intermediary for Weighing of Interests

The engagement of the PIMS as an intermediary for conducting the weighing of interests, required in the context of the possible ap-

plicability of the exemptions under Art. 17(3)(a) (Freedoms of Expression and Information) and Art. 17(3)(d) (Archiving in The Public Interest, Scientific or Historical Research Purposes or Statistical Purposes) has been considered as a possible service offering. It has, however, been concluded that while the exploration of such solutions would most certainly be in the interest of all involved parties, entrusting this task to Personal Information Management Systems would not be compatible with the established definition since it would require its extension towards other fundamental rights not related to the protection of personal data.[170] In the event that such a component was to be included in a PIMS or other type of platform, the exploration of the respective role taken towards the data subject might still be of interest.

First and foremost, it needs to be established to what extent the performance of such an assessment even requires the processing of personal data. After all, while the outcome would have a crucial impact on the rights and freedoms of the individual, it arguably comes closer to the provision of a legal analysis than a processing activity, per se. Since, however, the weighing of interests requires the consideration of the specific circumstances of each processing activity, including not only the interests of the general public and the controller in accessing the information but also the particular characteristics of the data subject including its position within society and the sensitivity of the information,[171] details relating to that individual will also need to be processed by the PIMS for the provision of such a service.

On the one hand, this processing could be qualified as commissioned data processing since the PIMS would essentially be taking

---

[170]See Part 1 Chapter 2: D. II. 3. b) bb) Reflections on Potential Advancements.

[171]Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 81: "*Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.*"

over a task normally falling under the responsibilities of the controller, thereby acting on their behalf. What stands in the way of such a qualification is, however, the requirement for processors to process personal data based on the controller's documented instructions, as established in Art. 28(3)(a) of the GDPR. Here, since the entire purpose of outsourcing the weighing of interest is the use of a third impartial and objective party, the PIMS would also need to be able to perform their analysis free from any influence of the controller, excluding the possibility of commissioned data processing in accordance with Art. 28. On the other hand, the assumption of separate controllership on the side of the PIMS, independently from the data controller, also does not seem possible since the processing of personal data relates to a direct legal obligation of the controller and is therefore inextricably linked to such. Based on that, the determination of the purpose of the processing will also essentially need to come from their side, whereas the PIMS will have to be left with the determination of the essential means of the processing. In that sense, the most logical outcome would be the assumption of joint controllership in the form of converging decisions which complement each other.[172]

c) Check-List

In the context of discussing commonly occurring practical hindrances and limitations in the complete removal of datasets from the controller's entire system, the possibility of submitting a form of "checklist" via the PIMS has been discussed (see Part 1 Chapter 2: D. II. 3. c) aa) Back-Ups). Such a documentation outlining the explicit modalities of the deletion process (Have you removed data from all back-ups? Have all copies been erased? Have all processors been informed of the request? Has the metadata related to the account been fully anonymised? etc.) could be used both as a form of quality assurance, as well as allowing the data subject to understand the specifics of the extent of the deletion. While the initial submission of

---

[172] *EDPB*, Guidelines 07/2020, para 53.

such a list does not constitute the processing of personal data, the answers provided by the controller to such will relate to the identified or identifiable individual as it provides details concerning the handling of their information. The parties will, however, not determine the means or purposes of such an activity jointly, nor will the PIMS be acting in accordance with the controller's instructions. Quite the opposite, they will in a sense be instructing the controller on behalf of the data subject. Such a list would also not be in any form binding upon the receiving entity. The extent to which the controller would act in accordance with the voiced demands would still depend on the modalities of Art. 17 and in that sense, not differ legally from simply submitting any type of data subject request via an intermediary. Based on that, the Personal Information Management System would need to be qualified as a separate controller, in the same vein as has been established in the context of the responsibilities for the submission of the individual's requests.

d) Expiration

As a result of the general problem of deleting personal data from the internet, which due to its open nature is considered virtually impossible, the idea of attaching an expiration date to a dataset which would ensure its automatic deletion, has been brought forward (see Part 1 Chapter 2: D. II. 3. c) bb) (1) Expiration). Examples include tools such as X-pire![173] (and its successor X-pire 2.0[174]), FADE,[175] EphPub,[176] the Ephemerizer,[177] or the Timed-Ephemerizer.[178] Since none of the publications concerning these solutions nor the role taken by such tools in the context of the processing of personal data has been mentioned, the question will be analysed independently herein.

---

[173] *Backes and others*, arXiv preprint arXiv:1112.2649.
[174] *Backes and others*, SAC '14, 1633, 1633ff.
[175] *Tang and others*, in: Sec. and Priv. in Comm. Net., 380, 380ff.
[176] *Castelluccia and others*, 19th IEEE, 165, 165ff.
[177] *Perlman*, 1 JISSec 2005, 51, 51ff.
[178] *Tang*, in: Public Key, 195, 195ff; *Tang*, 58 Comput. J. 2015, 1003, 1003ff.

As a first step, as always, the relevant processing activity will need to be identified in the context of the expiration functionality. On the one hand, the attachment of the expiration date to the dataset could be considered as such. On the other hand, however, it is at least questionable to what extent this information would actually be considered as personal data. While it does relate to a personal dataset, defining when such should be removed does not in itself relate to the individual and does not essentially entail any extra information independent from the underlying dataset. What does, however, constitute a processing activity is the deletion or anonymization of the data itself, as alteration, restriction, erasure, or destruction are explicitly mentioned as examples under Art. 4 No. 2. Where data has been transferred to other entities, this stage of the processing will also be conducted outside of their influence since the entire purpose of assigning an expiration date essentially lies in the avoidance of the current dependency on other parties to properly delete the relevant information. While other recipients might therefore be aware of the automatic expiration of a dataset, they can hardly be considered as involved in the "joint determination" of the purposes and means of the deletion, since all of these elements will be exclusively governed by the Personal Information Management System.

Equally, the PIMS will clearly also not be acting on behalf of any other data recipients, but rather based on the instructions and wishes of the data subject. As a result, the provision of an expiration functionality for the individual's datasets would need to be qualified as occurring under the separate controllership of the Personal Information Management System. This outcome would also be in line with the fragmented approach propagated by the CJEU, which explicitly allows for the division of the data lifecycle according to the specific stages of processing and a separate assignment of roles for the involved parties, with regards to such.[179] The outcome would be entirely different if a controller decided to commission a provider with

---

[179]For more details refer to Part 2 Chapter 3: C. III. 3. d) ff) Fragmentation and Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

the assurance of automated data expiration, as here the service provider would in fact likely be considered a processor. Such a service offering would, however, fall outside of the definitions of PIMS, applied at the heart of this thesis.

e) Revocation

The purpose of data revocation functionalities virtually mirrors those of expiration solutions in assuring the effective and complete deletion of datasets without being dependent on data controllers, holders, or other type of recipients. Whereas the expiration functionality will, however, in principle require the data subject to take privacy relevant questions into account prior to sharing their personal information, revocation services aim at allowing ad hoc deletion in instances where such a determination has not been initially made.

Part 1 of this thesis presented two solutions in that context: A system based on a caching mechanism of public Domain Name System resolvers that has the ability to refresh information over time while facilitating the expiration of its lifetime based on access novel heuristics called Neuralyzer[180] and a Data Revocation Service, offering the utilisation of unique data identifiers in order to solve the issue of locating datasets spread throughout the entire web.[181] The Neuralyzer essentially also offers a form of cryptographic erasure since the publicly accessible data is encrypted and the encryption key destroyed once the data subject requests deletion.[182] The second Data Revocation Service, on the other hand, does not directly interfere with the accessibility of the information but rather intends to notify controllers and processors of the current status of a dataset, for example, in the form of push and pull notices.[183]

Both the assignment of a unique identifier and the encryption of a dataset are most likely to be carried out in the form of a separate

---

[180] *Zarras and others*, in: Proceedings of the Sixth ACM Conference, 14, 14.
[181] *Kieselmann/Wacker*, 42 DuD 2018, 437, 438.
[182] *Zarras and others*, in: Proceedings of the Sixth ACM Conference, 14, 22.
[183] *Kieselmann*, Data Revocation, 14-17.

controllership in this context, as it will likely occur prior to any data transfers to other parties independent of their knowledge and out of their scope of control. The nature of this action, after all, largely mirrors the previously analysed expiration functionality. When it comes to the deletion or rather revocation of access to the dataset via the erasure of the encryption key or other identifier without the knowledge of the other controllers, the same is likely to apply. Where, on the other hand, the data has been transferred to another controller via the PIMS as part of a consent feature or other type of additional functionality, the parties are likely to determine certain parameters governing the processing of personal data, as well as the relationships between each other in advance. They are likely to be seen as joint controllers and the deletion of the dataset would then also presumably fall within the scope of this exchange.

Also imaginable are instances where the revocation would be connected to a feature where the PIMS takes the role of a processor on behalf of another controller. This was, for example, the case, in the context of cooperating platforms in which both data subjects and controller's sign-up for the services of the Personal Information Management System, as here the provision of a secure identification service for the individual users, has been qualified as a form of commissioned data processing (see Part 2 Chapter 4: D. I. 2. b) aa) Cooperating Platforms). Should a data controller, therefore, receive personal data through a PIMS and the use of such for the assurance of the individual's identity and furthermore request notifications or direct deletion of the information in question based on the preferences of the data subject in order to assure that their responsibilities in accordance with Art. 17 of the GDPR are met, the PIMS might after all be considered a processor rather than a separate or joint controller.

f) Interim Conclusions: Erasure

The above considerations essentially lead to the conclusion in the same vein as has been identified in the context of other functionalities: A uniform allocation of roles and responsibilities under the GDPR for the Personal Information Management System and the

data recipient, in the context of the provision of the right to erasure, is not possible. The submission of the demand of the data subject to one or multiple controllers occurs solely based on the decision of the data subject regardless of the recipients, leading to the qualification of the Personal Information Management System as an independent data controller for the related processing. The same classification will also apply to any sort of progress reports or statistics regarding the state of the requests, their success rate, or level of compliance provided to the individual user, as well as the submission of any type of "checklists" relating to the extent of the deletion. A separate controllership of the PIMS can also predominantly be assumed in the context of assuring the expiration of datasets where the act of erasure is qualified as a relevant processing activity, occurring outside of the scope of control of the other party, although the possibility of a controller-processor relation has also been left open in instances where a controller has requested the expiration of the data. Adding to the scope of possibilities, the provision of services allowing the flexible revocation of data has in fact been established as theoretically opening the possibility for the PIMS to take any of the three potential roles under the GDPR, depending on the related services and level of knowledge on the side of the data recipient. Last but not least, the idea of outsourcing the weighing of interests to a third, impartial and objective party, was considered. This functionality would be qualified as a joint controllership in the form of converging decisions which complement each other.[184] It has, however, been determined that it would not fall within the scope of PIMS, under the definition applied in this thesis, making its qualification irrelevant in this context.

4. Restriction

Article 18 of the GDPR provides the data subject with the right to restriction of the processing of their personal data in instances where (a) its accuracy is being contested; (b) the processing is unlawful; (c) it is no longer necessary for the original purpose; or (d) an objection

---

[184] *EDPB*, Guidelines 07/2020, para 53.

submitted to the controller under Art. 21(1) is pending verification. Based on this, it has been concluded that the right to restriction essentially constitutes an interim solution until the underlying conflict between the controller and data subject is resolved, rather than an independent right. The restriction of processing will, therefore, always need to be connected to the exercise of another type of right which might explain why at the moment there do not seem to be any service offerings on the market focussing on the assurance of such. As has, however, been determined under Part 1 Chapter 2: D. II. 4. c) bb) Potentials for Development, the inclusion of support in that regard could in fact be both relatively easy to implement as well as pose a significant advancement. The dataset—the status of which is still under determination—could, for example, be stored with the PIMS instead of the controller until the conflict is resolved. This would, on the one hand, reassure the data subject that no illegitimate processing activities are being conducted in the meantime, while at the same time alleviating the controller of the burden to separate and secure the relevant information.

When it comes to the designation of the proper role taken by the provider of such a service, with regards to the processing of personal data, referring to the respective designations in the context of data storage service offering may at a first glance seem sensible. There is, however, a crucial difference between a regular service offering for secure storage and the interim securing of a dataset. As outlined under Part 2 Chapter 4: A. Storage, Personal Information Management Systems deployed for the purpose of storing personal data by the data subject, either independently or in combination with other service offerings, will be qualified as (independent) controllers where the information is being held within their infrastructure. In contrast, no role will be taken by such in the context of local storage within the user's personal device. Whereas here the individual data subject is able to freely select the respective provider and the extent of their offerings, this will not equally apply in the context of the right to restriction. Although it falls under the category of data subject rights,

the right to restriction can be equally read as a responsibility to restrict on the side of the data controller. Where the accuracy of a dataset is being contested, it is no longer necessary for the original purpose of collection or the legitimate ground of the controller to require verification; the controller has a clear responsibility to cease the processing of the relevant information as outlined in Art. 18(2). In that sense, the storage of data requested by Art. 18(2), constitutes a legal obligation of the controller and is thereby inherently linked to such. A Personal Information Management System taking over such a responsibility will thereby evidently be acting on behalf of the controller, thereby making them the processor. This is also supported by the wording of Art. 18(1), which refers to the data subject's right to obtain restriction from the controller and not any other party or entity. Based on this, it can be concluded that while the individual might request the use of an intermediary for the storage in the context of restriction, the controller would not be obliged to grant such a request and essentially is left free to choose a service provider as they will also be liable for any misconduct of such.

5. Portability

As outlined in Part 1 Chapter 2: D. II. 5. Portability, this particular right applies in instances where (1) the data has been provided to the controller by the data subject; (2) the processing is performed by automated means; and (3) is based either on consent or performance of contract. This consists of two basic elements—the rights to receipt and to transmission—which can be realised though three actions. Individuals can receive their personal data directly, they are allowed to further transfer it to different entities, and where technically feasible, request the direct transmission from one controller to another. The data transferred to the individual or to another entity should be provided in an interoperable, structured, commonly used, and machine-readable format.

This right, which has been newly introduced the General Data Protection Regulation,[185] has the purpose of empowering data subjects through the ability to easily move, copy or transmit their personal data, as well as ensuring fair competition between controllers through the facilitation of a free flow of information.[186] In spite of its presumed practicability it has, however, not gained much practical relevance so far.[187] There are also a number of practical difficulties attached to its implementation such as the selection of the right format, as well as a number of security concerns relating to the fear of identity fraud and the threat of attacks performed on the data during transmission.[188] In light of its strong potential in the context of effective and efficient data sharing it has, however, unlike the previously discussed right to restriction, been subject of much interest in the context of Personal Information Management Systems, with many providers already offering or attempting to introduce portability functionalities. The analysis of the appropriate legal designation for such solutions should therefore begin with considerations on the existing service offerings before moving on to more theoretical divagations.

a) Existing Service Offerings

As outlined under Part 1 Chapter 2: D. II. 5. f) Practical Implementation, the service offerings currently available or under development can generally be divided into commercial solutions, which are endorsed directly by data controllers and such, which are offered by independent intermediaries. The ways in which these different types

---

[185] *Jülicher/Röttgen/v. Schönfeld*, 8 ZD 2016, 358, 359; *Dehmel/Hullen*, 4 ZD 2013, 147, 153; Kuner and others / *Lynskey*, Art. 20, 497, 500.

[186] *Art. 29 WP,* Guidelines on the right to data portability, 4; Ehmann/Selmayr, *Kamann/Braun*, Art. 20, para 2f; Kuner and others / *Lynskey*, Art. 20, 497, 499.

[187] https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/ (accessed 26 February 2026).

[188] *Scudiero*, 3 EDPL 2017, 119, 124f; Schwartmann/Jaspers/Thüsing/Kugelmann / *Rudolph,* 'Art. 20' DSGVO, para 72; Kuner and others / *Lynskey*, Art. 20, 497, 505; *Art. 29 WP,* Guidelines on the right to data portability, 19f.

of PIMS have defined their roles and responsibilities towards the data subject will be analysed herein.

It should also be noted that two providers, which also support the right to data portability, have already been examined in the context of data storage and consent functionalities above, namely MyDex and World Data Exchange.[189] In that sense, a reminder shall be sufficient at this point that MyDex has established itself as the "owner and controller of the data architecture of Mydex Master PDS Data Schema".[190] World Data Exchange however, does not reference their role taken in the context of the service offering in the Privacy Policy found on the website.[191] It has, however, been concluded that they likely have qualified themselves as a processor.

aa) Data Transfer Initiative

The Data Transfer Initiative, established in 2023[192] as a successor of the previous Data Transfer Project[193] and Data Portability Project,[194] aims at facilitating the downloading of data and its transfer between services.[195] At the time of writing, the main contributors were Apple, Meta and Google.[196] While the project does not consider itself a Personal Information Management System based on the fact that the information is stored within the originating service with destination services receiving a new copy, rather than connecting providers through the creation of an additional copy,[197] it has been

---

[189]See Part 2 Chapter 4: A. II. 3. d) MyDex and C. I. 2. World Data Exchange.

[190]MyDex Charter, https://dev.mydex.org/mydex-charter.html, (accessed: 14 March 2026).

[191]Word Data Exchange Privacy Policy, https://worlddataexchange.com/privacy-policy (accessed: 22 October 2025).

[192]Data Transfer Initiative, https://dtinit.org/ (accessed: 23 October 2025).

[193]ibid.

[194] *Auwermeulen*, 33 CLSR 2017, 57, 58; *Ursic*, 15 SCRIPTed 2018, 42, 46.

[195]Data Transfer Project Overview and Fundamentals, https://datatransferproject.dev/dtp-overview.pdf (accessed: 23 October 2025), 3.

[196]Data Transfer Initiative, https://dtinit.org/ (accessed: 23 October 2025).

[197]Data Transfer Intiative FAQs, https://dtinit.org/about (accessed: 23 October 2025).

established under Part 1 Chapter 2: D. II. 5. f) aa) Controller Endorsed Solutions that the initiative would still fall under the broad definition of PIMS put forward by the EDPS and applied for the purpose of this thesis.

With regards to the roles taken by the participants with respect to the data and vis-a-vis the data subject, the DTP Whitepaper differentiates between instances where the end user is the direct customer of one of the DTP services and such where an enterprise solution with a commercial customer is deployed.[198] Where the customer, thereby the data subject, has a direct relationship with the service provider, for example, in the form of a Gmail, Outlook or Facebook account, the DTP service naturally takes the role of the data controller, meeting their obligations in accordance with Art. 20 of the GDPR.[199] Such controllership is also completely separate from the other project partners who are not entitled to receive a copy or any access to the data.[200]

Where, on the other hand, the service of the DTP is being used by an enterprise in the context of their respective service offerings, the data subject will usually have a relationship with that party, typically either as an end customer or an employee of such. In such instances, the project specifies that since the commercial customer of the service takes the role of the data controller, the assurance of the right to portability in accordance with Art. 20 falls under their responsibility and they will thereby have the choice to either use the functionalities offered by the DTP for that purpose or select another solution.[201] Here, the DTP contributor will then take the role of a

---

[198]Data Transfer Project Overview and Fundamentals, https://datatransferproject.dev/dtp-overview.pdf (accessed: 23 October 2025), 7.

[199]ibid.

[200]Data Transfer Intiative FAQs , https://dtinit.org/about (accessed: 23 October 2025).

[201]Data Transfer Project Overview and Fundamentals, https://datatransferproject.dev/dtp-overview.pdf (accessed: 23 October 2025), 7.

processor in the same vein with regards to the service integrated with the DTP.[202]

bb) CozyCloud

Next to the features CozyNotes,[203] CozyPass[204] and CozyBanks,[205] the CozyCloud offers a CozyDrive which allows the automatic synchronisation of files on the user's computer with the cloud, the sharing of such data, and the automatic import from a list of more than 100 pre-defined providers.[206] The provider qualifies itself as a processor for all of these modalities, outlining in their privacy policy that the data subject exclusively determines the means and the purposes of the processing of their personal data and is therefore to be qualified to act as a data controller.[207] Additionally, they put an obligation on the end user to only use the cloud for processing of personal data "in the course of a purely personal or household activity" in the meaning of Art. 2(2)(c) GDPR, in order to assure that such falls under the household exemption.[208] The provider even goes so far as to require indemnification for any damages or fines from the data subject where this is not the case.[209] Putting aside the question as to whether or not a data subject could even legally be considered a data controller, which according to the view presented in this thesis is not the case (see Part 2 Chapter 3: A. I. 2. b) Data Subject), such a division or complete delegation of responsibilities on to the individual users does not seem particularly privacy friendly and could arguably exclude the provider from being considered a Personal Information Management System since the

---

[202]ibid.

[203]CozyNotes, https://cozy.io/en/#notes (accessed: 14 October 2025).

[204]CozyPass, https://cozy.io/en/features/#pass (accessed: 14 October 2025).

[205]CozyBanks, https://cozy.io/en/features/#bank (accessed: 14 October 2025).

[206]CozyDrive, https://cozy.io/en/features/#synchronise (accessed: 14 October 2025).

[207]CozyCloud Privacy Policy, https://cozy.io/en/policy/ (accessed: 14 October 2025).

[208]ibid.

[209]ibid.

data subject is essentially being burdened rather than supported in the execution of his or her rights.

cc) Citizen.me

In contrast to the more commonly used cloud storage solutions, Citizen.me opts for local data storage within the user's device.[210] The idea behind the "Zero-Party-Data" technology introduced by the provider, is the facilitation of access to data for companies and organisations which might request such directly from the data subject.[211] Such information is, however, supposedly "anonymised" by default.[212] The application supports the right to data portability by facilitating the initial gathering of data from various sources.[213] In their Terms of Service, from 2018, CitizenMe established that they may be qualified both as a controller and processor of the users' personal data (MeData).[214] These have, however, since then been removed from their webpage and not replaced as of October 2024. Furthermore, neither the Terms of Service nor the company's privacy policy specified which roles would be taken by the provider, under which circumstances, or for which specific element of the existing service offering.

dd) Personium

Personium offers a distributed Personal Data Store (PDS) server allowing for multiple applications and devices to access and modify

---

[210]CizitenMe, https://www.citizenme.com/ (accessed: 14 October 2025).

[211]ibid.

[212]The provider uses the term "anonymised form", it should however be assumed that this refers to the provisions of pseudonymised data, as anonymisation would most likely be next to impossible to achieve in this scenario. See: https://web.archive.org/web/20240519110736/https://www.citizenme.com/what-is-zero-party-data-zero-is-the-hero/ (accessed 25 February 2026).

[213]CizitenMe, https://www.citizenme.com/ (accessed: 14 October 2025).

[214]CitizenMe Exchange Terms of Service, https://web.archive.org/web/20240924145938/https://www.citizenme.com/citizenme-exchange-terms-use/ (accessed: 14 October 2025).

the contained data.[215] It is also intended to enable the secure sharing of data between connected data stores, allowing collaboration between multiple organisations and individuals.[216] As an example, the provider lists the option to allow a physician access to health-related data such as blood pressure measured previously by other parties or a private tutor accessing an individual's school records.[217] Unfortunately at the time of writing, neither the Terms of Service[218] nor the Privacy Policy[219] of the provider could be accessed, making it impossible to determine how the company's roles and responsibilities with regards to the connected processing of personal data were defined.

b) Legal Classification

A review of the existing solutions shows the importance of accurately and transparently defining the function taken by a Personal Information Management System. Each provider has largely taken a different view as to legal classification, with CozyCloud essentially transferring all responsibility onto the individual users, Personium not providing any determination, and solutions such as the Data Transfer Project, Citizen.me and World Data Exchange explicitly leaving open the possibility to either take the role of processor or controller, depending on the respective circumstances.

Regardless of the technical set-up of each system, two important characteristics which all tools supporting the individual's rights under Art. 20 have in common are: (1) they all require cooperation from the data controller, holding the information; and (2) tools assuring this right will not work independently from other functionalities such as storage or identify management. These two attributes essentially follow from the nature of the right itself. In order for such to be enacted,

---

[215]Personium, https://personium.io/en/index.html (accessed: 14 October 2025).

[216]ibid.

[217]ibid.

[218]Personium Terms of Service, https://personium.io/terms_of_service.html (accessed: 14 October 2025).

[219]Personium Privacy Policy, https://personium.io/privacy_policy.html (accessed: 14 October 2025).

the individual's personal data already has to be in possession of another entity (controller). Also, where the right is successfully enforced, the data will need to be transferred by this entity, creating the need for some form of data storage, either locally or in the cloud. These attributes are quite relevant in the context of the legal classification of the PIMS which should, however, be considered separately for the modalities of receipt and transmission, included the right to portability in accordance with Art. 20 of the GDPR.

aa) Receipt

Based on Art. 20(1), data subjects have the right to receive the personal data concerning them. Here, the Personal Information Management System could assist the individual in (1) submitting the request; (2) transferring the data from the controller to the data subject; and (3) safely storing the data on behalf of them. The role of a PIMS with regards to these activities has, however, already been considered in the context of other data subject rights, as explained previously.

The submission of the demand of the data subject to one or multiple controllers has already been discussed in the context of the right to access and rectification.[220] As outlined therein, the content of the individual's inquiry is related to that person and is therefore to be qualified as personal data in the meaning of Art. 4 No. 1. The transfer of this information to other parties therefore constitutes a processing activity, for which the PIMS will be considered an independent controller, since the submissions are being made autonomously from the receiving party and regardless of their legal status.

The possibility of ensuring secure transfers of personal data has also already been considered in the context of the right to receive a copy, included within the right to access.[221] Here it has been established that the Personal Information Management System would

---

[220]See Part 2 Chapter 4: D. II. 1. a) bb) Submission of Comfirmation and B. IV. 2. b) cc) (2) Automated Notifications Triggered by the Data Subject.

[221]See Part 2 Chapter 4: D. II. 1. c) aa) Security of the Copy.

need to be considered as a processor, since the obligation to implement appropriate technical and organisational systems falls under their scope of responsibilities in accordance with Art. 5(1)(f) and 32(1) of the GDPR and can therefore not be transferred onto another entity. In that sense, the selection of the PIMS by the data subject should merely be understood as a suggestion or communication of preferences. This does not, however, relieve them from their responsibility of due diligence, meaning that their agreement to the use of the PIMS can be considered equal to the deployment of a processor in the form of commissioned data processing.

Finally, the different forms of data storage have been analysed under Part 2 Chapter 4: A. Storage. In that context the conclusion was reached that where the personal data is locally stored within the user device, the Personal Information Management System will generally not take any function under the GDPR, since they are essentially only supplying the data subjects with a tool to process their personal data, similarly to a standardised software but are not directly involved in the determination of the means or purposes of the processing. In the context of cloud storage solutions, it has been concluded that while the customer is typically qualified as the data controller, with the cloud provider either taking the roles of a processor or at times joint controller, this assumption cannot be applied in the context of PIMS as it results in the data subject taking the role of controller for their own personal data. Since such an interpretation would negate the purpose of the GDPR of complete and effective protection of the individual, it should be assumed that a Personal Information Management System offering secure storage solutions to individual users is to be considered the controller for any type of information stored within their infrastructure.

bb) Transmission

Additionally, to requesting the receipt of their personal data in accordance with Art. 20(1) of the GDPR, data subjects also have the right to transmit this information to another controller without hindrance. Moreover, Art. 20(2) introduces the possibility of requesting

the direct transmission from one controller to another, where technically feasible. On the one hand, an analogy to the already discussed transmission of data to the data subject, for which the PIMS has been qualified as a processor, would seem plausible. On the other hand, however, instances of direct transmission to another controller also naturally lead to the emergence of another party, which might potentially change the dynamics of the situation. In that sense, the instances of indirect transmission under Art. 20(1) and direct transmission under Art. 20(2) should be explored.

(1) Indirect Transmission

In the case of indirect transmission based on Art. 20(1), the data subject would typically request that their personal data be submitted to them in a structured, commonly used, and machine-readable format and subsequently transfer such to another controller, based on their own preferences. Here, the Personal Information Management System can be deployed in order to assure the safe transmission of the information from the first controller to the individual, as well as for the subsequent transmission to the second data controller.

The role of the PIMS for the first part of the transmission has already been established in the previous section, as that of a processor acting on behalf of the transferring entity. This qualification, however, cannot be applied for the subsequent transmission from the data subject (or the PIMS) to the second controller. After all, here the GDPR only puts an obligation on the first controller not to create any hindrances for the data transfer but does not require any additional involvement. In that sense, the PIMS would not be taking over any of the controllers' responsibilities, nor acting on their behalf. The selection of the means by which the data should be transferred will be left completely to the data subject and the controller who initially provided the data, does not have any due diligence obligation regarding ensuring the implementation of appropriate technical and organisational measures by the PIMS, nor any actual influence over the submission itself. Consequently, the transfer of the dataset from the data subject (or from the PIMS where it has been stored there) to the sec-

ond controller needs to be considered as a separate processing activity for which an alternative division of roles and responsibilities needs to be applied.

The question of the role taken by the Personal Information Management System in the context of offering a secure channel for the transfer of the users' personal data, has already been considered with regards to the functionality of consent management.[222] Here, after all, the PIMS, will often not only be tasked with the collection and submission of the consent itself but the underlying datasets as well. It should, however, be noted that while the connection to consent is likely to occur most frequently in practice, the data subject will also be able to utilise a PIMS for the transfer of their personal data where a different legal basis for the processing by the receiving controller is applied. Imaginable are, for example, scenarios under which the individual wishes to enter into a contract with a new controller (Art. 6(1)(b) GDPR) or has a legal obligation to provide such with certain information (Art. 6(1)(c) GDPR).

Independently and arguably unrelated to the legal basis used for further processing by the receiving controller, the Personal Information Management System does, however, have its own legal basis for processing in the form of transmitting the individual's personal data which is most likely to be the performance of the service contract for use of the platform (Art. 6(1)(b) GDPR). The PIMS will also determine all of the essential means of the transfer, the security measures which are to be applied, and the form of submission, etc. The platform also has its own purpose for such processing, which is the fulfilment of the contractual (or other) obligations towards the user, which exists independently from the receiving controller.

On the other hand, the purposes and interest of the PIMS and the receiving controller seem to coincide to a certain extent. Art 5(1)(d) and (f) require any controller to ensure the accuracy, integrity, and confidentiality of personal data throughout the entire data lifecycle including its initial collection. In that sense, the relevant processing

---

[222] See Part 2 Chapter 4: C. II. 1. b) a) Of Datasets.

activity of the PIMS (submission) and that of the receiving controller (collection) overlap and create the obligation of ensuring the compliance with all modalities of Art. 5 on both sides, for the same act. Thus, the assumption of a common purpose and thereby a joint rather than separate controllership, might in fact be adequate. Such a reading would also be in line with the CJEU ruling in the case of Fashion ID where the website operator was also considered to be a joint controller with Facebook in the context of "the collection and disclosure by transmission of the personal data of visitors to its website" but not for any subsequent processing conducted by the platform.[223] Similarly, the PIMS and the receiving controller could be considered as jointly responsible for the collection and transfer of the users' personal data, while maintaining separate controllership for any prior or subsequent actions.

Such an outcome also seems sensible while taking into account that most of the actual commercially viable platforms allowing the management of consent, access, transfer, and portability all operate based on a cooperation with the service providers interested in accessing the individual's information.[224] Here the conclusions of a joint controller agreement in accordance with Art. 26, as part of the procedure of enrolling onto the platform, could be quite easily implemented. A question naturally occurs over how cases should be dealt with in which the PIMS only has a relationship with the data subject and does not in any way cooperate with other controllers. After all, it might seem problematic to essentially force a receiving controller into a joint controllership with the PIMS platform. It should, however, be noted that the party receiving personal data through such would still be aware of the involvement of the PIMS and could still object to the utilisation of such. Also, this scenario does not differ much from the

---

[223]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 76.

[224]See for example: Meeco, https://www.meeco.me/ (accessed 14 October 2025); MyDex Personal Data Exchange Services, https://mydex.org/platform-services/#_blank (accessed 14 October 2025); Digi.me Partherships, https://digi.me/partnerships (accessed 14 October 2025).

joint controllership assumed in the case of Fashion ID, where after all, Facebook did not have any influence over the form of data collection by the website operator. From a practical perspective, the PIMS would, however, likely be required to disclose the relevant details with regards to the transmission to the controller prior to its occurrence, which could effectively be achieved by submitting a drafter co-controller agreement to such.

(2) Direct Transmission

In addition to being allowed to further submit personal data received by one controller to another without hindrance in accordance with Art. 20(1), Art. 20(2) also provides data subjects with the right to have their personal data "transmitted directly from one controller to another, where technically feasible". While traditionally this obligation would be fulfilled by the controller it is, however, also imaginable for a Personal Information Management System to take over this task.

The analysis of instances of indirect transmission essentially led to a splitting of the activity into two separate modalities: (1) the transfer of the data set from controller one to the data subject or the PIMS; and (2) the transfer of the same, or a modified dataset, from the data subject or the PIMS to another controller. For each of these modalities, different roles were assigned to the PIMS. Applying these findings to instances of direct transmission is, however, quite problematic from a practical perspective, as there is no clear point at which the end of one action and the beginning of a second could be established. If the same rules were to be applied, an artificial demarcation line would essentially need to be agreed upon which would be quite difficult from a technical perspective as data transfers do not really allow for a division "in the middle", but rather constitute one seamless, undividable action.

Another problem relates to the inseparable connection of the obligation under Art. 20(2) to the first controller. Whereas in instances of indirect transmission, the responsibility of that party was limited to neglecting to create a hindrance, Art. 20(2) creates a direct legal requirement to act, which is inextricably linked to the controller in the same way in which the transmission of personal data directly to the

individual is made. In that sense, the legal qualification of the Personal Information Management System would also have to be identical as in the case of data transmissions to the data subject, making them a processor of controller number one. The role of a processor would in this case, however, be stretched for the transfer to the second controller as well since it constitutes one action that cannot be divided into two modalities.

While being the only sensible conclusion, this qualification as a processor of the PIMS directly transferring the individual's personal data from one controller to another raises the question of the relationship between the PIMS and the second controller. Whereas a joint controllership between the two has been established for indirect transmissions, this outcome seems in a sense impossible here, as it would make the PIMS a processor for one controller and a joint controller with another party for the same action. Also, since the first controller will be authorised to agree or reject the use of the PIMS as a transfer channel, they are inadvertently responsible for the determination of the means and purposes of the data transfer. This shift in reasponsibility does, however, have the effect that the Personal Information Management System will take a drastically different role based on whether the data subject decides to enforce their right to data portability through Art. 20(1) or (2) of the GDPR.

c) Interium Conclusions: Portability

While the right to data portability might not have initially gained much practical relevance immediately after the GDPR came into force, there seems to be a slow shift in that regard. This can particularly be observed in the context of the emerging service offering of Personal Information Management Systems, which quite frequently include functionalities directed towards the support of the right under Art. 20 of the GDPR. A look at the legal classification of the role under the GDPR taken by these providers, however, presents both a confusing and inconsistent picture I qualifying themselves as independent controllers, some as processors, and others completely neglecting to transparently define their role vis-a-vis the data subject. An

objective legal analysis of the different modalities of portability therefore seems imperative.

In the context of an individual's right to receive personal data under Art. 20(1), the PIMS could provide support in the form of a request submission, the transfer of data from the controller to the individual, and the subsequent storage of the information in question on their behalf. For the functionality of a request submission, the role as independent controller of the PIMS has already been established in the context of the right to access and rectification. When transferring personal data from the controller to the individual, the PIMS will, on the other hand, take the role of a processor, since they will be fulfilling a legal obligation inherently linked to the controller. In the context of storage, the role of the PIMS as an independent controller has also already been established.

Where personal data is indirectly transmitted to another controller in accordance with Art. 20(1) by the PIMS, the roles of the platform will be defined separately for the processing activity of transmitting the data to the individual user and subsequently transferring it to another controller. For the first, the platform will take on the role of processor as it is identical as discussed under the functionality of "receipt". For the second part, however, it should be qualified as a joint controller, with the party newly receiving the information as they are jointly responsible for the collection and transmission of personal data, analogous to the circumstances considered by the CJEU in the case of Fashion ID.

Such a division of the data transfer and thereby the roles taken in its context is not possible where the individual decides to exercise their right of direct transmission under Art. 20(2). While it obliges the controller where technically feasible to directly transmit the dataset to another party, this task might also be taken over by a PIMS. Here, however, the conducted data transfer will again be within the clear scope of responsibilities of the first controller, rendering the PIMS as a processor. As a result, if the current trend of assigning the roles under the GDPR on a "case-by-case" basis is to be followed consequently, the legal qualification and thereby the level of liability of the

Personal Information Management System will be drastically different for the different modalities of data portability outlined under Art. 20(1) and (2).

6. Objection

Finally, the individual's right to objection and the service offerings of the Personal Information Management Systems related to such should be discussed. As has been established in Part 1 Chapter 2: D. II. 6. Objection of this thesis, Article 21 introduces different types of instances under which the individual might object, with different rules applying to each of those.

a) Ordinary Objections

Article 21(1) regulates the ordinary objections to most types of processing activities. It stipulates that data subjects have the right to object to processing operations performed based on the legitimate interest of the controller, or on the necessity for the performance of a task carried out in the public interest, or in the exercise of official authority vested in such. Controllers are, however, not automatically obliged to cease the relevant processing operations but only where the individual in question can put forward grounds applying to their particular situation. These special circumstances will most likely relate to the weighing of interests, which need to be conducted when using the legal basis of Art. 6(1)(e) or (f).[225] The individual can therefore bring forward reasons based on which the performed analysis of proportionality should not be considered accurate for them.[226] If, on the other hand, the controller is able to demonstrate the presence of compelling legitimate grounds which override the interest, rights,

---

[225]Ehmann/Selmayr / *Heberlein*, Art. 6, para 46-53; Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 23, 29ff; Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 55ff.

[226]Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 19f; Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 9f; Kühling/Buchner / *Herbst*, Art. 21, para 15; LG Frankfurt, ZD 2019, 467, para 32.

and freedoms of the individual or the necessity of such for the exercise or defence of legal claim, they will be able to continue the processing activity in question.

aa) Pre-Confirmation

Before contemplating the submission of an objection to a processing activity, an individual would need to be aware of the fact that their personal data is being processed in the first place. In the context of the legal basis of legitimate interest and performance of a task in the public interest, this is, however, not necessarily a given. Whereas the natural person providing consent or entering into a contract will generally be aware of the collection and thereby further use of their personal data, the application of the legal basis of Art. 6(1)(e) and (f) will *often* lead to instances in which controllers might make general information about the purpose, type, and duration of their processing activities available through their privacy notice, without the individual person being able to ascertain whether or not their information in particular is also being used and to what extent. In that context, the right to access can indirectly support the right to objection, since Art. 15(1) allows data subjects to obtain a confirmation in that regard from the controller.

The interplay of these two rights can also be observed in the context of Personal Information Management Systems. As has been described under Part 1 Chapter 2: D. II. 1. a) bb) Pre-Confirmation, tools such as Revoke,[227] DeleteMe,[228] or Mine[229] are intended to support the rights of deletion and objection. Thus, they will, in the first instance, perform an analysis of the possible controllers holding information about an individual. This is, for example, achieved by means of searching the dark web, marketing databases, the individual's mailbox, or directly contacting data brokers.[230] To this end, a

---

[227]Revoke, http://revoke.com/ (accessed 22 February 2026).

[228]DeleteMe, http://joindeleteme.com/ (accessed 22 February 2026).

[229]Mine, https://www.saymine.com/ (accessed 22 February 2026).

[230]See for example: Revoke, https://revoke.com/pricing/ (accessed 22 February 2026); DeleteMe, https://joindeleteme.com/sites-we-remove-from/ (accessed 22

type of “pre-access” or “pre-confirmation” is performed in order to identify which entities might be worthy of contact. The performance of this analysis will in itself, also qualify as a processing activity, covering the steps of collecting data from the individual, consulting it with existing internal and external databases, and in the end, offering an overview of potential sources. This analysis is, however, conducted without the knowledge of and independently from the controllers, to which objections might later on be submitted. It is also presumably done for entirely different or even conflicting purposes than the ongoing processing activities of the other data controllers. The processing of personal data required for the provision of the “pre-confirmation” functionality is therefore conducted in the form of an independent controllership of the Personal Information Management System, which establishes both the means and the purposes for such.

bb) Request Submission

The same qualification as an independent data controller will also apply with regards to the subsequent submission of the individual’s objection to the processing of their personal data. Here, not only the individual’s preference (the cessation of the processing of their personal data), but also the particular circumstances of that person on which the objection is based, will be transferred to the recipient. This transfer will, however, in most instances be conducted without the initial knowledge or cooperation from the receiving controller.

A different legal qualification might apply in the context of previously discussed “cooperating platforms”,[231] where controllers signed up as commercial customers of the PIMS as well. In such instances where a business has previously agreed to receive requests for ob-

---

February 2026); Mine, https://www.saymine.com/transparency (accessed 22 February 2026).

[231] See Part 2 Chapter 4: D. I. 2. b) aa) Cooperating Platforms.

jection through the PIMS or might even have communicated a preferred form of communication with the platform, the submission might in fact also be considered as a joint controllership.

cc) Intermediary for Weighing of Interests

Since ordinary objections to the controllers' processing operations based on Art. 20(1) require the presence of grounds applying to the individual's particular situation, a sort of "re-weighing" of interests seems to be required. The legal basis of Art. 6(1)(e) and (f) already requires controllers to weigh their interest against the risks for the rights and freedoms of individuals related to the planned processing activity. Art. 20(1), however, allows data subjects to argue that this result is not accurate in the context of the specific circumstances applying to them.[232] Then again, controllers can still continue the processing of personal data where they are able to demonstrate compelling legitimate grounds which override the interests, rights and freedoms of the data subject. Considering the multitude of factors, elements and interests which need to be accounted for in the context of such a "re-weighing", the use of the Personal Information Management System as an objective intermediary to conduct such on behalf of the parties might be considered.

A similar type of functionality has already been contemplated in the context of the right to erasure, under Part 2 Chapter 4: D. II. 3. b) Intermediary for Weighing of Interests. While it has been established that there might be some doubts as to the extent to which an actual PIMS could in fact be fully objective, the possible division of roles should still be considered. This was previously achieved by way of exclusion. The function of a processor has been precluded based on the fact that it would entail the requirement to process personal data in accordance with the controller's instructions, which would go against the aim of using an impartial and objective intermediary. The

---

[232]Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 19f; Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 9f; Kühling/Buchner / *Herbst*, Art. 21, para 5; LG Frankfurt, ZD 2019, 467, para 32; Paal/Pauly / *Frenzel*, Art. 8 DSGVO, para 23, 29ff; Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 55ff.

role of a separate, independent controller was on the other hand denied, based on the fact that the weighing of interest and thereby the processing of personal data resulting from such, relates to a direct legal obligation of the controller and is therefore inextricably linked to them. Ultimately, a joint controllership between the commercial customer and the Personal Information Management System will thereby need to be assumed, as the first will predominantly determine the means of processing, whereas the latter is largely responsible for the purpose.

dd) Erasure Checklist, Expiration, Revocation

Where the data subject has effectively objected to the processing activity and the controller is unable to demonstrate legitimate grounds for its continuation, they are no longer allowed to continue to process the personal data of that individual in accordance with Art. 21(1). This essentially creates a requirement to erase the relevant dataset, since otherwise, even if it was only stored and not used for other purposes, the processing of such would still continue. In that sense, the successful exercise of the right to objection leads to the rise of the obligation for erasure. This fact is also directly acknowledged and supported by Art. 17(1)(c) which stipulates that data subjects can demand erasure where they have objected to *"the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)"*.

Since therefore erasure constitutes the logical consequence of any successful exercise of the data subject's rights under Art. 21, all modalities supporting the first will thereby naturally also assist the latter. In that sense, the previously analysed functionalities of providing the controllers with checklists, or ensuring the possibility of expiration and revocation of datasets, will be relevant here as well. Both the extent of these, as well as their legal qualification has, however,

already been discussed in detail.[233] A reminder should therefore be sufficient at this point that the PIMS will presumably take the role of an independent controller in the context of submitting any type of lists of questionaries, documenting the extent of the deletion. The same is likely to apply in the context of assuring the expiration of datasets where the erasure occurs outside of the scope of control of the other controller, whereas a controller processor relation might transpire in instances where a controller requested the expiration of the data. The most "flexible" when it comes to the qualification of the role taken by the Personal Information Management System, however, has been the provision of services allowing the flexible revocation of data, which have been established as theoretically allowing the presumption of any of the three potential roles under the GDPR, depending on the related services and level of knowledge on the side of the data recipient.

b) Objection to Direct Marketing

As established in Part 1 Chapter 2: D. II. 6. a) cc) Direct Marketing of this thesis, Articles 20(2) and (3) introduce a type of "privileged right to object" for instances where the objection concerns a processing activity conducted for direct marking purposes.[234] In this case, data subjects have the right to object at any time and once an objection has been submitted, processing for such purposes should be ceased automatically. The previously outlined conditions, such as the requirement for the existence of grounds relating to the particular situation of that individual or the need to consider compelling legitimate grounds overriding the interests of the data subject, on the other hand, do not apply.[235] It should, however, be noted that in contrast to Paragraph 1, Paragraph 3 does not create a requirement on

---

[233]See Part 2 Chapter 4: D. II. 3. c) Check-Lists, d) Expiration and e) Revocation.

[234]Paal/Pauly / *Martini*, Art. 21 DSGVO, para 47.

[235]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 518; *Art. 29 WP*, Guidelines on Automated individual decision-making, 19; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 44.

the side of the controller to completely cease the processing of the individual's personal data, but only to stop using it for the purposes of direct marketing, which means that further processing of the relevant information in another context will still be legitimate.[236] This will, in particular, cover the creation and maintenance of so called "Blacklists" which keep a record of individuals who have previously objected to the processing activity in question, in order to ensure that these are not repeatedly contacted.[237] In that sense, the previously discussed functionalities supporting the right to erasure will probably not be relevant in the context of objections under Art. 21(2) and (3).

Since, however, individuals do not need to meet any conditions or prove the existence of any particular reasons for their objection in the context of direct marketing, the application of so called "Do-Not-Track" functionalities has been discussed. These would entail an automated communication of the PIMS to the controller's system that the data subject objects to any tracking of their online behaviour either for advertising or for other purposes.[238] This idea is, in fact, not new since historically, various approaches have been taken in order to facilitate this type of functionality, including ideas such as the creation of a permanent opt-out cookie,[239] tracking protection features allowing the creation of blacklists and whitelists of websites,[240] or a HTTP header field sending out signals to website advertisers.[241] While in Part 1 it was concluded that considering the requirements of Art. 5(3) of the still applicable E-Privacy Directive Art. 21 cannot

---

[236]Kuner and others / *Zanfir-Fortuna*, Art. 21, 508, 518; Paal/Pauly / *Martini*, Art. 21 DSGVO, para 52.

[237]Gola/Heckmann / *Schulz*, Art. 21 DSGVO, para 23; Ehmann/Selmayr, *Kamann/Braun*, Art. 21, para 26; Kühling/Buchner / *Herbst*, Art. 21, para 32a.

[238]*Fairfield*, 11 Nw. J. Tech. & Intell. Prop. 2013, 575, 580; *Kamara/Kosta*, 6 IDPL 2016, 276, 276; *Cheng/Wang*, 19 JBEM 2018, 253, 257.

[239]Google Analytics Opt-out Browser Add-on, https://tools.google.com/dlpage/gaoptout?hl=en (accessed: 14 April 2026).

[240]*Kuhlmann*, 22 DePaul J. Art, Tech. & Intell. Prop. L. 2011, 229, 279.

[241]http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html (accessed: 25 February 2026).

be used as a legal justification for Do-Not-Track techniques, as these can only use consent under Art. 6(1)(a) as their legal basis for processing,[242] the legal role taken by such would still be interesting to consider. After all, various means of communicating the individual's preferences towards the controller could be used regardless of whether or not the full consequences of Art. 21 would in fact be enforced.

The communication of the user's preferences, set-up within the Personal Information Management System for other controllers, has in a sense already been considered in the context of consent. There the legal roles taken by the PIMS for submitting the consent signal have been analysed, whereas in the context of Do-Not-Track techniques, the submission of a "lack-of-consents" signal would constitute the relevant processing activity. These, however, can essentially be qualified as equal, as the underlying relevant information is essentially the same. In that sense, the discussed determination (see Part 2 Chapter 4: C. II. 1. b) bb) Of Consent) extends towards other types of preference communication. Thus, the PIMS submitting Do-Not-Track signals, whether through the maintenance of black and whitelists, HTTP headers, permanent opt-out cookies, or other technical means, should be qualified as controllers for the underlying processing of personal data. This controllership might be realised in the form of a separate controllership where the relevant data is submitted to the recipient without their prior knowledge and involvement. Where, on the other hand, the end controller has a contractual or other relationship with the PIMS or signs up onto the platform as well, the applicability of a joint controllership can be presumed.

c) Interim Conclusions: Objection

The right to objection essentially allows data subjects to communicate their preferences and particular circumstances to the controller in order to achieve the cessation of a particular processing activity on their side, where such is being conducted on the legal basis of

---

[242]Part 1 Chapter 2: D. II. 6. c) aa) (2) (a) Do-Not-Track.

legitimate or public interest. Based on that, the exercise of this right will in a sense always be founded on a disagreement of the individual with the action taken by the controller. In that context, the conclusion reached in this section, which predominantly assigned the Personal Information Management System supporting the exercise of that right, the roles of an independent controller, would seem quite logical. The PIMS will likely be qualified as such in the context or submitting requests and user-preferences, as well as conducting analysis of potential parties to be contacted, also referred to as a "pre-confirmation" functionality. Where, on the other hand, a weighing of interests would be conducted on behalf of the involved parties, the tool would have to take the position of a joint controller since the determination of the purposes still solely lies with the recipient of the request.

7. Interim Conclusions: Specific Considerations

While "data subject rights" are qualified as one type of claim with many common elements under the GDPR, the analysis of the particular forms of obligations related to such and how Personal Information Management Systems could support them has evidenced quite significant differences with regards to their legal qualification. Taking an overall look at the previously mentioned considerations, a general division into two types of rights could be introduced. One category, while still principally supporting the individual natural person in exercising their right, also directly or indirectly benefits the controller: The PIMS essentially takes over tasks which would otherwise fall under their scope of responsibility, potentially reducing their expenditures, as well as liabilities. Broadly speaking, this would apply to the rights of portability, rectification and restriction. Since these obligations are, however, so strongly linked to the person of the controller, they can only be "outsourced" to a certain degree, with the holder of the data still having to retain their position as a controller. Based on that, the PIMS will predominantly take the roles of a joint controller or processor in the context of assuring these types of functionalities.

The second category are functionalities related to rights which in a sense serve the purpose of rectifying a failure on the controller's part. This can be generally categorised as applying to the rights of access, erasure and objection.[243] The right to erasure, for example, essentially creates a legal basis for the data subject to "demand" the deletion of their personal data, although the obligation to do so would already be present at the time of request. In that sense, it is more of a reminder directed towards the controller concerning their duties. Similarly, the conditions for seizing the processing of personal data based on the individual's objection under Art. 21(1) would also already be present at the times of submitting a request, the controller might only not be aware of the particular circumstances applying to the individual's situation. Finally, the right to access could arguably be viewed as a form of rectifying a failure on the controller's side, to efficiently and accurately provide the data subject with the relevant information concerning the processing of their personal data, in accordance with the right to information under Art. 13 and 14. After all, the types of details to be provided under Art. 15(1), essentially mirror those listed in the previous two articles. This common element between the rights under Art. 15, 17 and 21 can also be observed in the qualification of their legal role taken under the GDPR. Here, since the Personal Information Management System will essentially be tasked with "taking over" an obligation which the controller arguably failed to correctly or completely implement, the PIMS is likely to be qualified as an independent controller for most functionalities related to these types of demands.

These categories only represent a general tendency, with the PIMS still being able to take a different type of role, depending on the

---

[243]While a data subject might exercise their right under Art. 16 as a result of a failure of the controller to correct the dataset in question, the intention of the right rather lies in the idea of keeping data up to date. In that sense, data subject requests under Art. 16 predominantly relate to changes in the individual's data (updating e-mail addresses, preferences or contact details) rather than to information wrongly collected by the data controllers, as here the right to erasure would be more likely to apply.

specific functionality and circumstances of the case. What should also be noted is that similarly to the general principles of data protection enshrined in Art. 5 of the GDPR, all of these rights are also in a sense intertwined with each other, meaning that the respective functionalities relating to one might at the same time support another right as well. For example, the creation of a link between the data stores of the PIMS and the controller, allowing the direct correction of changes to certain datasets across systems facilitating the right to rectification, could equally be used for the erasure of such. Similarly, all functionalities, assuring the deletion of personal data, will indirectly support the right to objection, since erasure constitutes the direct consequence of effective objection under Art. 21(1). In that sense, in practice it might be difficult to accurately take apart and categorise the different functionalities, the processing of personal data related to them, and thereby the respective roles taken by the Personal Information Management System towards the data subject. While the approach of accounting for all of the circumstances surrounding the relevant processing activity and determining the roles of the parties on a case-by-case basis is in line with the official guidance documents, the case law of the CJEU, and the prevailing academic opinion, it will in that context support a quite flexible division of roles and responsibilities with regards to the functionalities taken by a PIMS, possible leading to legal uncertainty for the parties involved.

E. Findings for Part 2

The purposes of this thesis lie in the determination of the roles under the GDPR taken by Personal Information Management Systems and the establishment of the respective responsibilities and liabilities resulting from such. Chapter 3 of Part 2 focused on defining

the various functions outlined within the GDPR and the legal obligations which are attached to those.

The central function is that of the data controller, which Art. 4 No. 7 defines as the party determining the purposes and means of the processing of personal data. This entity takes the main responsibility for the processing of personal data under their control, as it is their obligation to assure the compliance with all the requirements set out in the GDPR, while additionally having to be able to demonstrate this at any given time. They may also be subject to sanctions from the supervisory authorities and are potentially liable for any material or non-material damages incurred by a person as a result of an infringement of the regulation caused by them.

Where the means and purposes of processing are jointly determined by two or more controllers, they are considered joint controllers under Art. 26(1). In principle, all controllers are subject to all the obligations resulting from sole controllership under the GDPR but they are also required to allocate their respective responsibilities as controllers amongst each other, in the form of a contract. This contract, however, does not have an external effect, as supervisory authorities are in principle not bound by any of the terms of such agreements and may exercise any of their powers equally against any of the parties. Most importantly, data subjects may also claim full compensation against any of the joint controllers under the same conditions, which apply for single controllership. The effect of the agreement between the parties is therefore solely internal as the (joint) controller who has compensated the data subject for the entirety of the damages will, however, be entitled to claim back part of that compensation from the other controllers or processors, correspondingly to the level of responsibility each of the parties bears with regards to the infringement and the damages caused by such.

The processor is an entity which processes personal data on behalf of a controller, rather than for their own purposes. They should be acting based on the controller's instructions but may be given a margin of discretion in determining certain "non-essential" means of processing. Based on their general dependency on the controller,

their responsibilities and liabilities are also limited. While the GDPR does put certain direct obligations on them, such as maintaining a record of processing activities, implementing technical and organisational measures for the purpose of ensuring the security of personal data, notifying the controller of a personal data breach, and assuring an adequate level of protection for the personal data in the case of third country transfers, these do not exempt controllers of their due diligence in selecting such a provider. Also, while most of the sanctions which may be put on controllers by supervisory authorities also apply to processors, there are significant limitations in the context of liability for damages suffered by individuals under Art. 82, as processors can only be held liable where they have acted outside of or contrary to lawful instruction of the controller or where they have failed to comply with obligations under the GDPR specifically directed towards them.

The GDPR also establishes the roles of third parties and recipients. The first are defined in the negative as any natural or legal person other than the data subject, controller, processor, or individuals under their authority (Art. 4 No. 10). The latter is further defined as any natural or legal person to which personal data is disclosed (Art. 4 No. 9). There are, however, no obligations or liabilities resulting from these roles.

When establishing which role a specific party might take in the context of processing operations, there are certain crucial main elements which need to be accounted for. First of all, these are functional concepts, meaning that the determination of the respective roles should be conducted based on their actual influence and activities with regard to the processing of personal data and cannot be changed through formal designation which would contradict the factual circumstances. Secondly, the analysis of the parties' influence should be conducted on a case-by-case basis, taking into account all of the surrounding circumstances as well. Thirdly, the European Data Protection Authorities and the CJEU have established that the interpretation should also serve the general goal of ensuring effective

and complete protection of the data subject. As a consequence, especially the term “controller” is to be interpreted broadly. Finally, the ruling of the CJEU in the case of *Fashion ID* has introduced the idea of a phase-oriented approach, by which parties may take different roles in the context of different stages of an overall processing activity.

Based on all of these considerations, Chapter 4 has taken the various functionalities, both existing and theoretical, which may be offered by Personal Information Management Systems and meticulously applied the established framework in order to define the role which such a tool would take under the General Data Protection Regulation. The result of this analysis can probably best be described as diverse. Depending on the respective service offering, the relationship with the data subject and that with other controller, the PIMS could essentially take any of the roles defined within the Regulation. While they are most likely to be considered as controllers in the context of data storage conducted on behalf of the data subject, the PIMS might simply be considered a third party when providing a transparency-enhancing translation of another controller’s privacy policy. While they might be regarded as a processor when taking over the identification of the individual in the context of data subject requests or where they secure a dataset in the context of the individual’s exercise of their right to restriction, the PIMS might be considered a joint controller when ensuring the rectification of datasets through a predefined link with another controller or when acting as an intermediary in the weighing of interests.

These differentiations can even be observed within seemingly identical functionalities. An example of this is in the context of consent management. Whereas a PIMS will be considered a third party with regard to the intended end processing activity for which the consent is being provided, they will need to be qualified as a (sole) controller for the submission of a consent signal itself, while also potentially taking the role of a joint controller for the transfer of a dataset, based on such. In some instances, even the provision of the exact same service with differentiations only present on the technical level,

invisible to the average user, will cause a shift in legal designation. Whereas both in the context of direct rectification at the source and the creation of a link between datasets, the PIMS has been rendered as a joint controller with the entity processing the individual's personal data for their own purposes, the same will not apply when the PIMS is simply informing the other controller about the required changes via push and pull notices, as here they will be qualified merely as a processor.

This fragmentation of roles becomes even more severe when taking into account that the general goal of a Personal Information Management System should not lie in the provision of one of the functionalities discussed in Part 1 but rather in allowing the data subject complete and full control over their personal information. If therefore a provider actually offered a platform on which the data subject could store all of their information, manage their consent and the access provided to other controllers to such, receive an overview of the processing operations to which they consented, including any forward transfer and rectify, delete, restrict, and transfer all of that information across the board as a result of the phase-based approached introduced by the CJEU, the legal designation of the PIMS will essentially deviate for all of these elements. The PIMS might store the data as a separate controller, verify the individual's identity as a processor, transfer information as a joint controller, and be a third party for the information provided on the processing activities following such transfers. Later, they might again take the role of joint controller when directly rectifying the dataset, based on a pre-existing link, then take on the role of separate controller while submitting a request for erasure and that of a processor, while securing a dataset while its accuracy is being debated.

Taking into account that the legal designation of these roles is crucial when it comes to the determination of the obligations that a certain party has towards the data subject, as well as the extent of their liability for potential material and non-material damages caused by their misconduct, this fragmentation of roles essentially means that

not only will the PIMS formally take a different role vis-a-vis the data subject but the extent of their responsibilities and liability for potential damages will also vary for each of these services.

Further aggravating this situation is the fact that the respective designation of roles will not only depend on the technical configuration for the respective functionality but on the relationship between the PIMS and other controllers as well. Should a controller receive a data subject request through a platform, the PIMS will, in principle, be considered a separate controller. If, on the other hand the PIMS platform was set-up in a way which required the prior sign-up of the other controller, they will likely be considered as joint controller or even as being in a controller-processor relationship. In effect, the respective protection of the data subject will essentially be dependent on elements which are not even visible to the average user, namely the technical background and the legal relationship (or lack thereof) with another party.

Such a result can be described as not only missing the goal of complete and effective protection of the data subject but also severely lacking in transparency in accordance with Art. 5(1)(a) of the GDPR. Simply understanding the intricacies of the platform itself would seem to amount to a herculean task, requiring significant expert knowledge. This result cannot be considered as satisfactory considering these tools were intended to strengthen the individual's understanding of the processing concerning them, rather than cause further confusion and legal uncertainty. Also, while not the main concern, it should also be noted that this level of uncertainty might also affect the platform providers themselves who might be unsure which roles they should take and which obligations will apply to them as a result. After all, what is at stake is not just an understanding of the underlying processing operations but questions of liability as well. Since controllers and processors have both different legal obligations and different rules of liability for damages apply to them, data subjects might be faced with a paradoxical outcome under which they may claim compensation from the PIMS for a malfunction on one

functionality but not another. Such a result could simply not be intended by the lawmakers and most certainly not by proponents of further developing Personal Information Management Systems, which is why the final part of this thesis should focus on the search for alternative legal interpretations and solutions.

Part 3

Return to Reason: Alternative Interpretations and Forms of Liability

Considering the conclusions reached in Part 2 of this thesis alternative forms of interpretation or deriving liability for PIMS should be considered. This is not only essential for the protection of the individual user, but also for the purpose of ensuring legal certainly for all involved parties. After all, providers of Personal Information Management Systems might be reluctant to create new innovative solutions, if the extent of their legal obligations is unclear. If PIMS are truly to realise their potential in empowering individuals in the control of their personal data, a clear and transparent framework for their functioning needs to be ensured. This Part will therefore explore the available options, for the creation of such. As a first step, the possibility of limiting the concept of PIMS, in order to achieve a more coherent legal designation will be considered (Chapter 5). Secondly, alternative rules, regulations, and obligations, which might apply to PIMS outside of the GDPR will be analysed (Chapter 6). Finally, alternative forms of interpretation, in the context of assigning the roles under the GDPR to the parties, will be presented, in an attempt to alleviate the identified problems (Chapter 7). Based on these findings the necessity for a new Regulation for PIMS will be explored (Chapter 7 D.).

Chapter 5

Limitations of the PIMS Concept: Towards a New Definition

Section A of Part 1 of this thesis established that no uniform definition for the concept of "Personal Information Management System" exists at the time of writing. The same term is also frequently used in other contexts such as human resources, compliance, or for the description of regular organisers. There is also no common definition for any of the other concepts used to describe these types of privacy enhancing technologies such as "personal data spaces", "stores and vaults",[1] "privacy management tools",[2] "data dashboards",[3] "data boxes",[4] or "data cockpits".[5] These denominations are at times used interchangeably as synonyms, while at other times in order to differentiate between them.

While this thesis applied the definition established by the European Data Protection Supervisor who described PIMS as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data",*[6] which is also most commonly used and accepted within general literature concerning

---

[1] *Lehtiniemi*, 15 S&S 2017, 626, 626ff; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

[2] *Datenethikkommission*, Gutachten, 133.

[3] *Attoresi/Moraes*, TechDispatch #3/2020, 3.

[4] *Crabtree and others*, 4 J Reliable Intell Environ 2018, 39, 39ff.

[5] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024).

[6] *EDPS*, Opinion 9/2016, para 4.

the subject,[7] this characterisation is inherently broad and includes a potentially unlimited number of service offerings with significant variations, both regarding their technical functioning and the relationships between the parties involved. The wide range of the term can be evidenced alone by the literature and discussions included in Part 1, which essentially sets out to provide a generalised overview of possible potential service offerings. Still, while not intending to be complete, the analysis can be described as relatively extensive.

It should, therefore, come as no surprise that the range of potential legal designations is just as wide as the range of the possible service offerings. Hence, one remedy for this legal uncertainly could be the limitation or specification of the terminology. The delineation of more concrete characteristics required for a system to fall under the concept of a "Personal Information Management System" (or any other selected term for that matter) could contribute significantly to establishing a more uniform regime of controllership and liability for these tools. This, in turn, creates questions as to both the content of these restrictions and the form in which they could be introduced.

A. Content

Specifications regarding the extent of the term "Personal Information Management System" could be introduced both in relation to the technical and the personal sphere.

---

[7] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

I. Technical Sphere

On the technical level, a clearer definition of the functionalities, both required or not covered by the term PIMS, is imaginable. The Data Governance Act, for example, introduced the term "data sharing services" and Art. 9(1) specifically sets out what type of service offerings fall under its scope.[8] Furthermore, Art. 11 provides for certain conditions under which these services should be operated, including such relating to the technical sphere. For example, Art. 11(2) specifies that metadata collected in the context of providing data sharing services may only further be used for the purpose of its development. Art. 11(4) also defines the format in which data should be exchanged, namely that per default, the format in which it was received from the holder should be used but that conversion into other formats might be allowed where this serves the enhancement of interoperability.

Also providing a quite clear definition for *Services for Consent Management* (Dienste zur Einwilligungsverwaltung) is § 26 of the German Telecommunications Digital Services Data Protection Act (TDDDG),[9] where platforms with their own commercial interest in the

---

[8] These are: (a) intermediation services between data holders which are legal persons and potential data users; (b) intermediation services between data subjects that seek to make their personal data available and potential data users and (c) services of data cooperatives.

[9] Please note: the German Telecommunications Telemedia Data Protection Act (TTDSG) came into force in December 2021 and was then replaced by the Telecommunications Digital Services Data Protection Act (TDDDG) in May 2024. There were however no changes within the here referenced paragraphs. The sources in the below sections may therefore refer to the TTDSG, instead of the TDDDG, while still remaining valid. See: Bundesgesetzblatt, 'Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze', https://www.recht.bund.de/bgbl/1/2024/149/VO (accessed 24 October 2024).

user's consent (§ 26(1) No. 2 TDDDG) or own underlying interests in the processing activity (§ 26(1) No. 3 TDDDG) are explicitly excluded from the scope. While the term "Personal Information Management System" is at no point used within the Act, the academic literature has predominantly subsumed these services under that term.[10] Also, although no specific requirements regarding the type of storage, confidentiality, integrity, availability or resilience, as outlined under Part. 1 Chapter 2: A. Storage have been introduced, § 26(1) No. 4 TDDDG does require the submission of a security concept. Introducing even more specific restrictions would be imaginable across the board of all available PIMS service offerings.

1. Interference

As has been outlined under Part 2 Chapter 4: B. I. 3. Recommendations, the provision of a recommendation by the transparency enhancing tool for alternative service providers was associated with a significant shift in influence over the final processing activity. The shift occurred since the PIMS essentially created the possibility for the processing to take place, thereby leading to joint controllership. This type of functionality could arguably also be seen as an interference into the individual's decision-making process, who is essentially being steered towards the selection of a different provider. The intent of effecting the individual's selection can, for example, be clearly observed in the Usable Privacy Policy Project, where the possibilities of nudging users into making more privacy friendly choices have been contemplated, based on observed differences between ex ante and ex post user preferences.[11] If, however, any type of interference, whether in the form of providing recommendations, warnings or even "gentle" nudging were to be prohibited by introducing a type of "neutrality requirement" for the platform, then this differentiation in roles taken by the PIMS depending on functionalities would not occur. In

---

[10] *Kühling/Sauerborn*, 11 ZD 2022, 596, 596; *Kühling/Sauerborn*, 10 ZD 2022, 531, 531; *Piltz*, 8 CR 2021, 555, 563; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 7.

[11] *Sadeh and others*, Usable Privacy Policy Project, 13.

the same vein, introducing a complete opposite stipulation into the definition of PIMS could also be considered, for example, by requiring platforms to actively support the data subject to make more privacy friendly choices. The effect would essentially be the same, as the type of role the PIMS might take towards the data subject would be more clearly established, extensively limiting the possibilities of shifts and variations in the responsibility of different platforms.

2. Storage Types

Also associated with a noticeable shift in responsibility were varying storage solutions, primarily the difference between local and cloud storage. While in the first case the PIMS will not take any role under the GDPR, the second will at least cause the PIMS to take the role of a processor and, based on the opinion voiced in this thesis, even a controller. Again, the pre-definition of the type of storage required by such systems would significantly limit the risk of emerging differences in liability. Also, imaginable and most likely quite valuable would be specifications regarding the security solutions necessary for these tools, for example, in their required resilience, availability, integrity and confidentiality settings. Such specifications could cause a significant improvement regarding consumer protection. Since the standard user might not have the technical knowledge to understand relevant differences in the measures implemented by different providers, the establishment of certain minimal technical security requirements would certainly be in the interest of these data subjects.

3. Access

Closely related to the question of storage type and the connected technical settings is the question of the extent to which the Personal Information Management System has access to the individual user's personal data. As has been mentioned while reviewing the various offerings currently available on the market, many providers operate based on a "zero-knowledge" policy, meaning that the PIMS itself

does not have any access to the user's personal data.[12] While the assumption that a lack of access would also make the service provider a third-party intermediary rather than a controller or processor in their own right, which is frequently argued by such providers, was disputed (see Part 2 Chapter 4: C. II. 2. a) Access), it is without a doubt that the question of access, or lack thereof, can still have a relevant effect on the role taken by such tools. A pre-defined stipulation of a "zero-knowledge-policy" could therefore be considered as both privacy-friendly solutions, as well as adding to the overall legal certainty in qualifying the tools' role under the GDPR.

4. Setting of Preferences

Another imaginable qualification could relate to the question of what type of preferences can be established within the settings and by whom. While discussing the right to rectification, different forms of informing the controller of the need to adjust a certain dataset were considered. With automated notification, a significant shift in responsibility, as well as the legal designation of the parties, was observed based on whether the notification would be triggered by the data controller or the data subject.[13] The same has also been concluded for the right to erasure[14] and objection.[15] This makes sense, since the determination of the systems settings essentially equals "control" of the related processing of personal data in the form of determining its means. If therefore, the configuration of preferences and events causing for example notifications or changes within datasets where

---

[12] *European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016) 11; Mydex, Achieving Transformation at Scale, https://mydex.org/resources/papers/AchievingTransformationAtScale/ (accessed: 24 October 2025).

[13] See Part 2 Chapter 4: D. II. 2. c) Automated Notification.

[14] See Part 2 Chapter 4: D. II. 3. e) Revocation.

[15] See Part 2 Chapter 4: D. II. 6. a) dd) Erasure: Checklists, Expiration, Revocation.

exclusively left to the data subject, the possibility of the “end controller” taking a more prevalent role within the PIMS would be significantly reduced.

5. Minimal Extens of Services

Another important finding established in Part 2 (see Part 2 Chapter 2: E. Findings for Part 2) regarding the role taken by the Personal Information Management System under the GDPR is the influence of different combinations of service offerings on the overall role taken by the tool. Since the determination of the function assumed by an entity under the GDPR should be made on a case-by-case basis, taking into account all the surrounding circumstances, the consequence is naturally that the presence of or affiliation with other components would also have a strong effect. In that context, a shift of responsibility has for example been observed in secure identification functionalities for which the PIMS will not take any role under the GDPR where they function as a stand-alone service but might in fact act as a processor where the offering is combined with other available features.[16] Pre-defining the possible combinations of service offerings, for example, as minimal requirements which would need to be present in order for a tool to fall under the scope of Personal Information Management Systems, would therefore certainly support more legal certainly in that regard. Such a delimitation would also add to the overall transparency of these services, both in the sense of data privacy but also consumer protection. After all, the currently observed free use of various denominations can be seen as a significant hinderance in allowing individuals to understand the extent of the selected services or the differences in relation to other providers.

6. Existing Limitation

The relevance and potential effect of a pre-defined scope of functionalities can in fact be observed in one of the functionalities consid-

[16]See Part 1 Chapter 2: D. I. 3. a) Identification of a Link.

ered in Part 1 of the thesis. The possibility of using the Personal Information Management Systems platform as an intermediary for the weighing of interests is required, for example, when exercising the data subject's right to erasure or objection. While the potential role taken by such an intermediary (joint controller) was examined, it was most importantly concluded that Personal Information Management Systems would per definition not be able to take such a role, as they would need to consider fundamental rights in general and not just the individual's right to privacy, making them more than just *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*.[17] Based on that, the potential role taken by the PIMS was essentially limited by the applied definition itself, proving the effectiveness of such delineations.

7. Interim Conclusions: Technical Sphere

To avoid the problem of shifting responsibilities within one Personal Information Management System, the introduction of limitations within the technical sphere might be considered. A standard for the type of data storage or the level of access granted to the service provider might for example be applied. Also, the question of whether the PIMS should be interfering with the individual's decision-making process (for example in the form of nudging for the selection of privacy friendly options or offering alternatives) should be addressed. As a result, the roles and responsibilities of the different actors would be more clearly defined. Furthermore, it might be advisable to actually define a minimal extent of service offerings which need to be available in order to fall under the definitions of a PIMS. This would solve the current problem under which tools with drastically different functionalities are potentially covered by the existing terminology.

---

[17] See Part 1 Chapter 2: D. II. 3. b) bb) Reflections on Potential Advancements.

II. Personal Sphere

While limitations regarding the technical functioning of these platforms certainly have the potential to reduce the variations in roles taken by the parties, regulating the personal sphere, specifically the relationship between the parties would likely have an even more meaningful effect. It has, for example, been established for the functionality of secure identification that there is a significant difference in legal classification of independent platforms which function with no support from the controller and cooperating platforms to which the parties interested in receiving personal data also need to sign up.[18] A similar differentiation was also observed in the right to revocation (see Part 2 Chapter 4: D. II. 3. e) Revocation) and consent (see Part 2 Chapter 4: C. II. 1. b) Collection and Transmission). The different roles of controllers, processors, joint controllers, third parties and recipients serve the explicit purpose of depicting the various functions taken by the entities involved in the processing operation, as well as the relationship between them. Therefore, in order to divide their responsibilities and the extent of their liability in a fitting manner, it makes sense that pre-defining certain modalities of these relations for the term PIMS would naturally limit the amount of potential outcomes. As a result, potential forms of limiting the terminology in that regard should be explored.

1. Relation with the Controller

An example of such a limitation can be found in § 26(1) No. 2 of the German TDDDG. Here, additionally to the already mentioned exclusion of own commercial interests, it is established that recognised consent management platforms need to be independent from the undertakings which might have such interests. While the extent of this independence is not further specified, it would at least require them to be a separate legal entity.[19] Any solutions endorsed directly by the

---

[18]See Part 2 Chapter 4: D. I. 2. b) Identification of the Data Subject.
[19]Assion / *Aretz*, § 26 TTDSG, para 44.

data controllers who also wish to further process it for their own purposes, such as those presented in the context of data portability under Part 1 Chapter 2: D. II. 5. f) aa) Controller Endorsed Solutions, would therefore be excluded. It can also be presumed that any economic dependence such as the financing or promotion of data controllers of such platforms, as well as investments or other types of support granted by such, would also exclude the possibility of being considered a recognised consent management platform.[20] In that sense, the German lawmakers seem to be inclined to support solutions offered by non-profit organisations and foundations, rather than commercial businesses.[21]

This limitation can in fact have quite a significant effect. As has been established for the analysed, currently available service offerings aimed at consent management, the solutions which are most mature from a commercial perspective largely depend on the cooperation of the data controllers who have an underlying interest in the individual's data (see Part 1 Chapter 2: C. V. Interim Conclusions: Consent). This identified dependence can materialise in different forms.

a) Dependence of the Data Subject

With Meeco, it has been determined that while the platform allows for the set-up of the digital-vault, directly by the end user, doing so would require a substantial amount of technical knowledge (see Part 1 Chapter 2: C. IV. 4. Meeco). Also, the intention of the platform seems to be the set-up by the data controller rather than the individual itself. This dependence, however, exists between the data subject and the controller, rather than the controller and the PIMS, meaning that this would not fall under the restriction of § 26(1) No. 2 TDDDG.

Although not falling under the existing restriction of the German TDDDG, this type of limitation could still be considered. After all, a

---

[20]Assion / *Aretz*, § 26 TTDSG, para 44; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 24.

[21]*Piltz*, 8 CR 2021, 555, 563; Assion / *Aretz*, § 26 TTDSG, para 44.

dependency of the use of a Personal Information Management System on the data controller interested in the processing of the data subject's information, can raise questions regarding the requirement of consent to be "freely given". If the support of a controller was necessary in order to sign-up to the platform, the argument could be made that the data subject is essentially paying such an entity for their technical support with their personal data. While the general concept of using personal data as a form of payment for seemingly "free" services is neither new or illegal,[22] its validity should be seriously questioned in PIMS which are intended to introduce more control for individuals into the sphere of their personal data management. The extension of the requirement for such platforms to function independently from other controllers, to the relationship between the end recipient and the data subject, would therefore seem reasonable.

b) Dependence of the Platform

With World Data Exchange and MyDex the dependence occurs in the form of the necessity for the controllers to also sign up to the platform as users, in order for the data subject to manage their consent preferences for such an entity (see Part 1 Chapter 2: C. IV. 2. World Data Exchange and 3. MyDex). *While* these are therefore both instances in which the PIMS platform itself essentially depends on the participation of the end controllers in the platform, there are still some differences in the applied models.

aa) Financial Dependence

While certainly intended to support individuals in the exercise of their rights, MyDex arguably stands somewhere between a compliance tool and a data subject focussed solution. While underlining the importance of enabling individuals to control their data, they also fre-

---

[22] *Hacker*, Datenprivatrecht, 53; *Elvy*, 117 Columbia Law Rev. 1369, 1384-1386; *OECD*, The App Economy, 25.

quently refer to the benefits of their Platform Services for organisations.[23] Companies interested in cooperating with the platform and setting up access accounts for individuals are also required to pay substantive fees outlined in the provider's pricing document.[24] While this does not create a direct reliance as it would be the case if one of the end recipients was an investor or holding company of the PIMS, the fact that fees are collected from controllers does create an economic connection. If the platform's revenue depends on the interest of other data controllers in such, there is a certain amount of pressure on the PIMS to be beneficial for their business customers as well. After all, if the platform failed to support companies in collecting consent or ensuring data subjects' rights, they might be inclined to look for alternative providers. In turn, the PIMS might be compelled to influence the user's behaviour in the interest of their paying customer in order to remain commercially profitable, thus failing their primary goal of supporting the data subject. The exclusion of any scenarios under which there is any dependence of the PIMS, financial or otherwise, on the data controller, will also largely limit the possibilities of the occurrence of a controller-processor relationship which is inherently characterised by the reliance on the controllers' interests and instructions.

bb) Dependence on Cooperation

Where there is no direct economic dependency, platforms such as World Data Exchange[25] might still be "dependent" on businesses, in the sense that individual users can only set-up their privacy preferences within the platform for the existing "brands". While certainly not at the same level as receiving financial benefits from the business

---

[23]Mydex, https://mydex.org/platform-services/#personal-data-store (accessed: 24 October 2025).

[24]Mydex Personal Data Stores - Pricing Summary, https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92698/195947716718579-pricing-document-2020-07-19-1041.pdf (accessed: 24 October 2025).

[25]World Data Exchange, https://worlddataexchange.com/ (accessed: 24 October 2025).

users, this could still to a certain extent affect the interests pursued by the platform. While ideally the immense popularity among data subjects would urge businesses to join the platform in order to support them in the access of new data sources, this might be a double-edged sword. After all, the interest of the data subject wishing to manage their privacy preferences via such a platform will also depend on the extent to which this can practically be done. If only a very limited number of businesses were to cooperate with such a platform, the time and effort put into the management of one's preferences might be deemed unproportionate to the actual benefits received. Especially new platforms which are still under development and fighting for market relevance will certainly feel the need to ensure cooperation with as many business users as possible in order to remain competitive. This dependence on the cooperation of end controllers has the potential to affect the autonomy of the Personal Information Management System and should therefore ideally be avoided. If in fact any type of cooperation between the PIMS and a data controller were to be excluded as per definition, this would also largely eliminate the possibility of the occurrence of a joint controllership, which requires the existence of a communal decisions-making power between the parties (see Part 2 Chapter 3: C. II. 3. Joint Determination of Means and Purposes).

2. Relation with the Data Subject

Additionally, to setting up rules governing the connection and level of dependency between the PIMS and the data controller, the relationship between the PIMS and its end user could also be defined. § 26 of the already mentioned German Telecommunications Digital Services Data Protection Act, for example, states that consent management platforms are not allowed to have their own commercial interests in the provision of consent or in the managed data (§ 26(1) no.2), nor for that data to be used for any other purposes than consent management (§ 26(1) no. 3). A similar restriction can be found in Art. 11(1) of the Data Governance Act, which specifies that *"the provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users and data sharing services"*. As a result, the roles which might be taken by the

PIMS vis-à-vis the data subject are limited as they will essentially be excluded from being a controller for anything else other than the management and submission of the consent signal, since any other underlying interest is per se excluded. The PIMS' role as a processor is also excluded through the prohibition of own commercial interests, as such interest would be impossible to avoid if they were acting on behalf of another controller.

This is just an example and alternative forms of governing the relationship between a Personal Information Management System and the data subject might be considered, especially in relation to other functionalities. For example, the previously mentioned "zero-knowledge" policies[26] excluding any access of the PIMS to the individual's data while relating to the technical sphere, could also be introduced on a personal level. Similarly, the question of recommendations and nudging users into certain choices could be excluded through a neutrality requirement or introducing an obligation of non-interference.

The opposite form is, however, also imaginable. In particular, this is true when managing data subject requests for access and portability where the substantial amount of administrative hurdles, as well as the reported frustration of users with the entire process, was described. Data subjects might therefore in fact be interested in appointing the PIMS as a type of "trustee" entrusted with the collection and administration of the individual's data. Data sharing services under the Data Governance Act, for example, are not set-out as inherently neutral, at least in their relation to the data subject as Art. 11(10) explicitly required providers to *"act in the data subjects´ best interest"*. This includes the provision of advice on potential data uses, as well as the terms and conditions attached to such, thereby introducing a form of "recommendation functionality". The same could also be considered in consent management. Since the actual validity of

---

[26] *European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016) 11; Mydex, Achieving Transformation at Scale, https://mydex.org/resources/papers/AchievingTransformationAtScale/ (accessed: 24 October 2025).

consent is often questioned and users tend to be fatigued with the excessive amount of notices they are being presented with, the question occurs whether the PIMS could answer such requests for the data subject based on certain pre-determined settings. To what extent such an outsourcing would, however, be legally admissible is still subject to much debate, as the requirements for consent to be informed and specific would likely not be met.[27] Regardless, defining the relationship between the user and the PIMS, e.g., whether the provider would act as an agent, trustee, representative or intermediary, would allow a far more precise determination of their roles taken under the GDPR.

3. Interim Conclusions: Personal Sphere

While more specifically defining certain technical elements required for a service to be considered a PIMS has shown some effect on limiting the potential variations in the roles taken by the parties, regulating the relationships between the parties would likely be even more effective. This is because the difference between separate controllership, joint controllership, and a controller-processor relationship often does not predominantly lie in the actual technical set-up but rather the agreement between the parties (see for example Part 2 Chapter 3: B. II. 2. c) Indicators for Delimitation). Does one party provide instructions? Who makes the decisions regarding the means and purposes of processing? Do the parties agree on certain elements together or do they work independently? All of these questions relate more to the relationship between the actors, rather than the actual technical details of the processing activity. For example, in the context of both consent management platforms and such supporting the exercise of other data subject rights, the question of the relation between the PIMS and the other controller will be crucial in determining its legal status. Should the PIMS act on behalf of such a controller, they would be deemed a processor. If they cooperate with them, they might be a joint controller, whereas independence from other

---

[27] *Botta*, MMR 2021, 946, 948f; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 10; *Kühling/Sauerborn*, 10 ZD 2022, 531, 532f.

parties would most likely amount to a separate controllership or result in being considered a third party. For example, § 26(1) No. 2 of the German TDDDG introduced such a requirement of independence in the context of consent management platforms, which means that any controller endorsed solutions will not fall within the terminology.[28] A similar solution could as well be considered for PIMS. Also relevant is the relationship between the platform and the data subject. Most importantly, it needs to be determined whether PIMS are acting in a neutral manner or should rather be actively guiding data subjects towards more privacy friendly solutions.

B. Form

While introducing a more specific definition for the term "Personal Information Management System" would certainly contribute to the establishment of a more uniform regime of controllership and liability for these tools, the question occurs how such a classification could be formally achieved.

I. Specification by the EDPS and other Bodies

The terminology as well as the notion of Personal Information Management Systems created in order to support the individual data subject in the realisation of the right to self-determination has been solidified in the mainstream consciousness of privacy professionals as a result of the Opinion of the European Data Protection Supervisor published in 2016,[29] and shortly followed by the report of the European Commission.[30] Subsequently, many publications dealing with

---

[28]Assion / *Aretz*, § 26 TTDSG, para 44; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 24.

[29]*EDPS*, Opinion 9/2016, para 4.

[30]*European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016) 11.

the same notion picked up the term, leading to its general acceptance.[31] It could be considered whether the EDPS should also take the lead in specifying the terminology through a new publication. However, even if the EDPS published specific criteria for Personal Information Management Systems, the extent to which this would successfully limit the current disarray is at least questionable. The simple publication of an Opinion does not lead to any binding consequences for providers, meaning that the term could still be freely used by businesses not meeting the outlined criteria. After all, as has been delineated in the beginning of this thesis, the designation "Personal Information Management System" has in fact been used for a long time in other areas such an in the context of organisers, as well as human resources and compliance. It is still applied in these contexts. It is therefore unlikely that a simple clarification by the EDPS would have a significant impact on market realities which already use the term interchangeably with other designations such as personal data spaces, stores and vaults,[32] privacy management tools,[33] data dashboards,[34] data boxes,[35] or data cockpits.[36] The same would likely also apply if any other body such as, for example, the European Commission, the European Data Protection Board or the Supervisory Authorities attempted to define the term more strictly by issuing a publication.

---

[31] *Horn/Riechert/Müller*, in: Neue Wege, 7, 8; *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026); *Kühling/Sauerborn*, 11 ZD 2022, 596, 596; *Kühling/Sauerborn*, 10 ZD 2022, 531, 531.

[32] *Lehtiniemi*, 15 S&S 2017, 626, 626ff; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

[33] *Datenethikkommission*, Gutachten, 133.

[34] *Attoresi/Moraes*, TechDispatch #3/2020, 3.

[35] *Crabtree and others*, 4 J Reliable Intell Environ 2018, 39, 39ff.

[36] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024).

II. Specification through Codes of Conduct

While simply adapting a previously established definition might not add any relevant legal certainty, the possibility of introducing more standardised rules through codes of conduct might be considered. Codes of Conduct are a form of "self-regulation" for entities.[37] Under Art. 40(2) of the GDPR, associations and other bodies which represent groups of controllers or processors may prepare such codes in order to specify how compliance with the Regulation is being assured. The areas which may be covered are listed in an exemplary manner in Art. 40(2) GDPR and include rules on fair and transparent processing, how personal data is being collected, procedures for pseudonymisation, the management of data subject requests, the transparent provisions of information, or the assurance of appropriate safeguards for transfers to third countries.[38] The idea behind the establishment of such rules comes from the inherent vagueness within the GDPR.[39] Since data protection law covers such broad areas relevant to all parts of our lives, controllers and processors dealing with similar types of processing activities are given the opportunity to establish more precise rules, relevant to their field.[40] If the codes of conduct proposed by the specific group are approved by the supervisory authority or the Commission, they serve as a form of guarantee for the entities who have committed themselves to ensuring that their processing operations comply with the GDPR.[41]

It is imaginable that providers of Personal Information Management Systems would form an alliance or association and agree on certain procedures. While the code only concerns the compliance of their processing with the Regulation, it may have an indirect effect

---

[37] *Wolff*, 4 ZD 2017, 151, 151; *Drobek*, 2 GIS Odyssey Journal 2022, 129, 131.

[38] *Roßnagel* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 40 DSGVO, para 38-49; *Drobek*, 2 GIS Odyssey Journal 2022, 129, 134.

[39] *Bergt*, 10 CR 2016, 670, 670f; *Wolff*, 4 ZD 2017, 151, 151.

[40] *Wolff*, 4 ZD 2017, 151, 151; Gola/Heckmann / *Lepperhoff*, Art. 40 DSGVO, para 1.

[41] Ehmann/Selmayr / *Schweinoch*, Art. 40, para 5; Gola/Heckmann / *Lepperhoff*, Art. 40 DSGVO, para 5; *Vander Maelen,* 6 EDPL 2020, 231, 237.

on the terminology as well. First, the establishment of a code of conduct would require that these entities see themselves as one category of controllers or processors. As has, however, been outlined in Part 1 of this thesis, there are significant differences in the ways these various services function. Should a specific type of PIMS establish a code of conduct, the term would possible be associated with such and in a sense "monopolised" by them. Other types of services would not technically be prevented from using the same denomination but might be more inclined to defer to a different terminology in order to differentiate themselves. While not resulting from the enactment of codes of conduct, such a monopolisation has in fact happened in Germany where the term "PIMS" is predominantly used in reference to consent management platforms.[42]

III. Specification through Certifications

Another alternative which relates closely to codes of conduct would be a potential specification through introducing certifications. In contrast to codes of conduct, the creation of certification mechanisms is out of the hands of the controllers or processors.[43] In accordance with Art. 43(5) GDPR, they need to be issued either by accredited certification bodies or by a competent supervisory authority. They are also not limited in their applicability to certain groups of controllers and processors or specific types processing activities, industries, or economic sectors.[44] Where a controller or processor has demonstrated compliance with the GDPR, the certification would be issued for a specific product or service.[45] Therefore, the same certification could be used for demonstrating compliance by any service provider, including PIMS.

---

[42] *Kühling/Sauerborn*, 11 ZD 2022, 596, 596; *Kühling/Sauerborn*, 10 ZD 2022, 531, 531; *Botta*, 12 MMR 2021, 946, 946.

[43] Sydow/Marsch / *Raschauer*, Art. 42, para 9.

[44] Sydow/Marsch / *Raschauer*, Art. 42, para 8; *Scholz* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 42 DSGVO, para 21f.

[45] Gola/Heckmann / *Lepperhoff*, Art. 42 DSGVO, para 9; *EDPB*, Guidelines 1/2018, para 4.

The establishment of a certification mechanism would therefore not really support the limitation of the term PIMS in any manner. The only imaginable form would be if a specific certification for Personal Information Management Systems was to be created. After all, certifications for certain economic sectors, for example, for IT providers, have already been established and the EDPB has explicitly supported the notion of more targeted mechanisms.[46] While not directly limiting the term, defining certain common rules and criteria might lead to some standardisation. Obtaining certification is entirely voluntary (Art. 42(3) GDPR), meaning that even if a PIMS-specific certification existed, providers would not be required to adhere to it.[47] Still, their possession could constitute a significant economic advantage, creating an important incentive.[48] On the other hand, there seems to be a risk for commercial certification providers to be more "inclusive", in the sense of allowing all types of service offerings into the scope, as this would certainly be more profitable for them. Based on this, mechanisms offered by supervisory authorities should probably take preference.

IV. Specification by Means of Recognized Services

Worthy of mention in that context is again § 26 of the German TDDDG, which introduces a form of accreditation for "recognised" consent management services. § 26(1) TDDDG provides the general requirements applicable to such service offerings and then further states that these may be recognised by independent bodies. § 26(2) TDDDG then clarifies that the Federal Government should enact a law specifying how these tools should work (§ 26(2) No. 1 TDDDG) and the necessary technical and organisational measures (§ 26(2)

---

[46] *Scholz* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 42 DSGVO, para 9-11; *EDPB*, Guidelines 1/2018, 58.

[47] Sydow/Marsch / *Raschauer*, Art. 42, para 11; Ehmann/Selmayr / *Will*, Art. 42, para 20; *EDPB*, Guidelines 1/2018, 5.

[48] *Scholz* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 42 DSGVO, para 4; Sydow/Marsch / *Raschauer*, Art. 42, para 19.

No. 3 TDDDG). Most importantly, however, it asks for the establishment of a procedure for their recognition (§ 26(2) No. 2 TDDDG). This official recognition could be read as a form of "certification" supporting the validity of a specific service offering.

The law outlining this procedure, referred to as the "Consent Management Regulation" (Einwilligungsverwaltungsverordnung – EinwV), has been enacted in September 2024.[49] The accreditation procedure is outlined in Part 3.[50] Service providers will need to apply for recognition (§ 11(1) EinwV) with the German Federal Commissioner for Data Protection and Freedom of Information (§ 8 EinwV). The application needs to include a description of the service, evidencing that the requirements set out in Part 2 of the Regulation are met (§ 11(2) EinwV), as well as a Security Concept (§ 11(4) No. 2 EinwV). Once the DPA has recognized a service, they will be listed in a public registry (§ 13 EinwV).

While the Regulation has been subject to much debate and criticism prior to enactment,[51] it does evidence the potential of such accreditation and certification mechanisms. The main problem of the newly introduced regulation on consent management is not the form of accreditation but mainly the fact that they are restricted to collecting consent for the storage or access to information stored in the terminal equipment of the user, based on Art. 5(3) of the ePrivacy Directive.[52] Consent in the meaning of Art. 4 No. 11 GDPR can, how-

---

[49]BT-Drs 20/12718, Verordnung nach § 26 Absatz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und zur Änderung der Besonderen Gebührenverordnung Telekommunikation (4 September 2024)

[50]*Nebel*, 16 ZD-Aktuell 2022, 01321.

[51]*Hanloser*, 8 ZD 2023, 421, 422; *Schmitz*, 14 ZD-Aktuell 2023, 01304; *DSK*, Stellungnahme: § 26 Abs. 2 TTDSG, 1ff.

[52]*Hanloser*, 8 ZD 2023, 421, 421; *Nebel*, 16 ZD-Aktuell 2022, 01321; *Schmitz*, 14 ZD-Aktuell 2023, 01304; *DSK*, Stellungnahme: § 26 Abs. 2 TTDSG, 2; *Kühling/Sauerborn*, 10 ZD 2022, 531, 532.

ever, not be legally obtained based on the requirement of being "specific".[53] Here a EU-wide extension of the concept of "broad consent" would likely be required to allow actual, effective consent management in that form.[54] Still, the idea of accreditation has a great deal of potential. Additionally, to building user trust,[55] this type of approval by the DPAs, can also effectively be used in order to provide a more specific requirement for the functioning of such service offerings. Similar mechanisms might therefore be considered on an EU level.[56] This is especially important since differences within Member State accreditations (or lack thereof) may again hinder the free flow of data within the EEA.

C. Towards a New Definition

There are certainly various ways in which the definition of Personal Information Management Systems might be adjusted in order to achieve more consistency as well as legal certainty. Next, the question as to which of these solutions should in fact be supported needs to be raised. It is the opinion presented here that both on a technical as well as a personal level, the PIMS should not interfere with the decision-making process of the individual. Users should therefore not be nudged into the selection of more privacy friendly options. Rather, information should be presented impartially with a focus on the individuals' preferences. Through that, the individual's right to self-determination will be supported to the fullest extent. Furthermore, this should be independent from any outside influences

---

[53] *Hanloser*, 8 ZD 2023, 421, 421; *Schmitz*, 14 ZD-Aktuell 2023, 01304; Assion / *Aretz*, § 26 TTDSG, para 17; different opinion in: Geppert/Schütz / *Schmitz*, TTDSG §26, para 7-13; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 16.

[54] *Hanloser*, 8 ZD 2023, 421, 421; Assion / *Aretz*, § 26 TTDSG, para 17; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 16.

[55] *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, 6 MMR-Beil 2021, 25, 32; *Hanloser*, 8 ZD 2023, 421, 422; Assion / *Aretz*, § 26 TTDSG, para 26.

[56] Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 4.

and should include both the end controllers, as well as any other interest groups. Such a restriction would not only further the interests of the individual user but also essentially exclude the possibility of a PIMS taking the roles of a data processor. Finally, while the specific elements included within a service offering do not need to be predetermined in a detailed manner, the term PIMS should generally be reserved for holistic platforms supporting the management of the entire data lifecycle. A simple cloud storage provider should not be considered a PIMS, neither should tools only focused on the submission of erasure requests or the interpretation of privacy policies. While such technologies may also support the individual in certain aspects of managing their data, the definition would simply become bottomless if every tiny functionality providing any type of support would automatically amount to a PIMS. After all, while the formal definition established by the EDPS is quite broad,[57] it does seem as though the general intention was supporting holistic platforms which include elements such as consent management, portability and even personal data analytics.[58]

It would be my suggestion to slightly amend the existing definition, thereby providing a more precise and narrow scope of service offerings falling within the terminology. Based on the previous considerations, this definition could read as follows: “Personal Information Management Systems are technologies and ecosystems which operate in an independent and neutral manner to support individuals in the control, collection, and sharing of their personal data throughout the data lifecycle”. Through this slight specification, the three most relevant criteria which have caused significant shifts in the roles and responsibilities taken by the PIMS would be pre-determined. Firstly, the requirement for data to be managed throughout the data lifecycle eliminates platforms which include singular functionalities that have only a limited effect on the actual data management and thereby often take the role of third parties, such as purely transparency en-

---

[57] *EDPS*, Opinion 9/2016, para 4.
[58] ibid 15-17.

hancing tools or sole storage solutions. Secondly, the element of independence eliminates the possibility of cooperation with other data controllers and thereby essentially excludes the option of a PIMS taking the role of a data processor or even joint controller. Finally, the element of neutrality ensures that the data subject is not steered towards any type of behaviour, further excluding any relevant influence on processing activities outside of the platform. The new definition would therefore lead to a more consistent and uniform approach to PIMS, resulting in higher levels of transparency and protection for the consumer.

D. Interim Conclusions: Limitation of the Concept

The assignment of different roles under the GDPR for varying functionalities of Personal Information Management Systems has been identified as a significant problem in Part 2 of this thesis. In order to mitigate this issue, different alternatives are considered in Part 3. One suggested possibility would be the limitation or specification of the term. This could lead to a more coherent outcome in establishing the responsibilities and liabilities of PIMS providers. Such a specification could relate both to the technical set-up of the platform and the relationship between the different parties.

On a technical level, establishing a prohibition of interference or suggesting any action to a user might be considered. Also possible would be a determination as to the storage type which should be used or whether the PIMS itself would have any access to the user's personal data. Another solution would be determining admissible combinations of service offerings in advance, for example, by setting up minimal requirements to be met in order to fall within the term "Personal Information Management Systems". Finally, it might be reasonable to decide what type of preferences can be established within a platform and by whom.

On a personal level, both the relationship of the PIMS with the data subject, as well as other controllers, could be regulated. Considering that the aim should be the empowerment of the individual, it seems reasonable to require platforms to be independent from other

controllers. Based on that, service offerings financed by other data controllers or requiring their cooperation could be excluded. In relation to the data subject, it should be determined whether the PIMS should take a non-partisan role, neither recommending nor discouraging any action, or rather be more of an active advisor or trustee.

Another question is how the considered restriction of the terminology could be achieved under current law. One option would be a specification by the European Data Protection Supervisor, whose *"Opinion 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data"* supports the current broad understanding. Similarly, bodies such as the European Commission, the European Data Protection Board, or the Supervisory Authorities could attempt to define the term more strictly by issuing a publication on the matter.

A potentially limiting effect might also be introduced through the establishment of codes of conduct and certifications. In order to agree on a code of conduct, PIMS providers would have to see themselves as one category of controller or processors in the first place and thereby define certain criteria for their functioning. Similarly, the creation of a specific certification applicable to PIMS could lead to a higher level of standardisation. Unfortunately, none of these solutions has the potential to create an actual binding effect. They might, however, indirectly lead to more transparency, as well as conformity.

Chapter 6

Liability Outside of the GDPR

The previous section focussed on providing suggestions for a more coherent form of liability for Personal Information Management Systems by limiting the current broad meaning of the term. It is, however, also of interest to look outside of the regime of the GDPR for alternative rules, regulations, and obligations, as well as forms of liability for Personal Information Management Systems. This may in fact be particularly relevant considering the amount of new laws recently created by the EU. It should, however, be noted that this section will solely focus on legislation applicable at an EU-wide level and not discuss alternative forms of liability in national laws.

A. E-Privacy Direcitve

Probably closest to the GDPR in services as well as activities covered is Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) also, referred to as the ePrivacy Directive. The connection between the two Acts is in fact directly recognised in Art. 95 of the GDPR, which states that it *"shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC"*. This means that where similar obligations already exist for a specific entity under the ePrivacy Directive, such as

for example the notification of breaches, the same action will not have to be duplicated for the purpose of complying with the GDPR.[1]

Similarly, Art. 1(2) of the E-Privacy Directive provides that its provisions *"particularise and complement Directive 95/46/EC"*. As a result, the ePrivacy Directive takes precedence as *"lex specialis"* where it provides more specific provisions for otherwise generalised rules established in the GDPR.[2] Processing operations not governed by the Directive will, however, still fall under the stipulations of the Regulation.[3] The term "complement" refers to instances where the ePrivacy Directive extends the scope of the GDPR.[4] This is, for example, the case in Art. 1(2) ePrivacy Directive, which extends the purpose to also protecting legitimate interests of subscribers who are legal entities. [5]

I. Applicability

Article 3 of the ePrivacy Directive provides that it applies *"to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices"*.

While a definition of electronic communication services has not been included in the ePrivacy Directive, it can be found in Directive 2002/21/EC of the European Parliament and of the Council of March 7, 2002 in a common regulatory framework for electronic communications networks and services referred to as the "Framework Directive". Based on Article 2(c), therein an electronic communication service covers any type of offering which is provided for remuneration and is wholly or mainly established for the conveyance of signals on electronic communications networks. The term includes telecommunications services and transmission services in networks used for

---

[1] *EDPB*, Opinion 5/2019, para 44.
[2] ibid para 38.
[3] ibid para 38.
[4] ibid para 42.
[5] ibid para 42.

broadcasting. Information society services (as defined in Art. 1 of Directive 98/34/EC), as well as services which exercise editorial control over the transmitted content are, however, excluded. The same definition can also be found within other acts of EU law such as for example Art. 1 No. 3 of Commission Directive 2002/77/EC of September 16, 2002 on competition in the markets for electronic communications networks and services or Art. 2 No. 4 of Directive (EU) 2018/1972 of the European Parliament and of the Council of December 11, 2018 establishing the European Electronic Communications Code.

1. For Renumeration

The first characteristic can be easily confirmed for most standard, commercial offerings provided for some type of fee. It might, however, not be the case for all Personal Information Management Systems, since some might be provided free of charge. Here it needs to be considered that Art. 2(c) of the Framework Directive only asks for services to "normally" be provided for remuneration. A singular service provided for free (for example in order to generate an initial user base or to gain market relevance) will therefore still fall within the term if most offerings in the sector require a payment by the user.[6] Additionally, the CJEU has in the context of defining "Information Society Services" explicitly supported a broad understanding of the term also including economic activities remunerated through other parties or means.[7] This might, for example, be the case where a service is provided without charging the recipients, but where revenue is being

---

[6]Assion / *Assion*, § 3 TTDSG, para 75; Grabitz/Hilf/Nettesheim */ Randelzhofer/Forsthoff*, 'AEUV Art. 56, Art. 57', para 46; Taeger/Gabel / *Arning/Rothkegel*, Art. 4 DS-GVO, para 499.

[7]C-339/15 *Vanderborght* [2016] ECLI:EU:C:2016:660, para 36; C-291/13 *Papasavvas* [2014] ECLI:EU:C:2014:2209, para 26; Case C-484/14 *Mc Fadden* [2016] ECLI:EU:C:2016:689, para 41; Case 352/85 *Bond van Adverteerders* [1988] ECLI:EU:C:1988:196, para 16.

generated through advertisements.[8] In that sense, even PIMS offered to data subjects without a direct payment are likely to fall under that definition, since they will typically charge the controllers or have a different business model, allowing them to profit economically in some form.[9] Potentially excluded might, however, be sole pro-bono or research projects such as Advanced Data Protection Control.[10]

2. Conveyance of Signals

Furthermore, the service needs to consist wholly or mainly in the conveyance of signals via electronic communications networks. This will include all types of offerings focused on facilitating the sending of electronic signals for the purpose of communication through means such as phone lines, satellite cables, satellite networks, or internet connections.[11] Consent Management functionalities and those related to the facilitation of data subject rights can certainly be considered as "conveying signals". In consent management, this will be the user preference which is being communicated to the data controller. For the exercise of data subject rights such as access, erasure or portability requests, an even higher level of communication between the data controller and the data subject would be facilitated by the PIMS platform. Even transparency related functionalities could technically fall within the scope if, for example, the PIMS provided a "translation" or "interpretation" of a specific policy submitted by the controller to the affected individual.

---

[8]C-291/13 *Papasavvas* [2014] ECLI:EU:C:2014:2209, para 30; Case C-484/14 *Mc Fadden* [2016] ECLI:EU:C:2016:689, para 43; Case 352/85 *Bond van Adverteerders* [1988] ECLI:EU:C:1988:196, para 16.

[9]*Spindler*, 4 GRUR 2021, 545, 547; *Janal*, 2 ZEuP 2021, 227, 234.

[10]Advanced Data Protection Control, https://www.dataprotectioncontrol.org/ (accessed 23 October 2025).

[11]Schumann/Mosbacher/König / *Gerhold/Handel*, § 1 TMG, para 7; Heermann/Schlingloff / *Bähr*, § 2 UWG, para 279; Hoeren/Sieber/Holznagel / *Schmitz*, 'Teil 16.2 Datenschutz im Internet' in Thomas Hoeren, Ulrich Sieber and Bernd Holznagel, HdB MultimediaR, Teil 16.2, para 126; Loschelder/Danckwerts / *Erdmann/Pommerening*, § 36 Nachricht, para 13; Harte-Bavendamm/Henning-Bodewi / *Keller*, § 2 UWG, para 162.

What is unclear, however, is to what extent the services provided by Personal Information Management Systems do in fact "wholly or mainly" consist of the conveyance of these signals. On the one hand, holistic platforms offering the management of one's entire data lifecycle will not have their main focus on the submission of content or signals. On the other hand, the various elements of a PIMS platform might also be considered as separate services, especially if they can be subscribed to or purchased independently from each other.[12] Such a separation is, for example, accepted for service providers offering both internet access and Voice over IP-Services or service portals.[13] As a result, consent management or other features facilitating the communication with the data controller might be considered as electronic communications services, independently from other functionalities.

Another hurdle could be the exclusion of services which provide or exercise editorial control over the transmitted content. Traditionally this exception refers to offerings such as radio, TV-programmes or online newspapers. [14] Arguably, the support provided to individuals when facilitating the exercise of data subject rights such as access, rectification, erasure or portability is likely to include the exercise of some form of editorial control. After all, the idea behind these types of functionalities is essentially that the PIMS would take over the often lengthy and cumbersome communication with the data controller from the data subject, in order to unburden them from this task. In the suggested "request specification" (see Part 1 Chapter 2: D. II. 1. c) cc) Request Specification), the data subject is likely to communicate their preferences toward the PIMS, which will afterward "take over" the assertion of these rights on the individual's behalf.

---

[12]For example, World Data Exchange offers various features, which can also be selected independently from each other. See: World Data Exchange, https://worlddataexchange.com/features (accessed 23 October 2024).

[13]*Martini/von Zimmermann*, 23 CR 2007, 427, 428; Schumann/Mosbacher/König / *Gerhold/Handel*, § 1 TMG, para 8.

[14]Heermann/Schlingloff / *Bähr*, § 2 UWG, para 279; Loschelder/Danckwerts / *Erdmann/Pommerening*, § 36 Nachricht, para 11; Harte-Bavendamm/Henning-Bodewi / *Keller*, para 162.

This applies even more to the discussed possibility of "auditing" controllers' answers for completeness and correctness, prior to forwarding such to the affected individual (see Part 1 Chapter 2: D. II. 1. b) cc) Perspectives for Advancement). Here the PIMS will be directly involved in the content of the transmitted information as they will communicate any shortcoming towards the controller and directly ask for corrections to be made with no involvement from the data subject. Similarly, they might edit the answer for the data subject. Especially in an access request, directed toward the receipt of details about the processing activity, the PIMS might edit the controllers' reply into a more standardised or easily understandable form, similar to transparency enhancing functionalities applied for presenting privacy policies. The provided service will therefore not be "wholly or mainly" focused on the pure conveyance of signals as the PIMS is likely to be actively involved in the content of the transmitted information.

Closest to a pure conveyance of signals are consent management functionalities. Here the Personal Information Management System is likely to only transfer the consent signal or other type of preference of the user. Also possible, especially in combination with storage functionalities, would be the direct transmission of the individual's personal data. This would, however, only require a form of "forwarding" and not include any type of editorial or other involvement of the PIMS in the signal's content or data in question. However, since both existing Personal Information Management Systems, as well as such under development, are internet based the actual consent signal is still formally being conveyed by the Internet Access Provider, with the PIMS only serving as an intermediary entity between data subject and controller. An analogous problem has already been subject to proceedings before the CJEU. The case of *Google LLC* dealt with the question whether or not the web-based e-mail service "Gmail" offered by Google constituted an electronic communications service.[15] Here the Court concluded that the fact that the provider actively participates in sending messages through actions such as the

[15]Case C 193/18 *Google LLC* [2019] ECLI:EU:C:2019:498, para 25.

assignment of e-mail addresses, splitting the messages into data packets, or uploading them was not sufficient for them to be considered as "wholly or mainly" consisting in the conveyance of signals on electronic communications networks.[16] This conclusion was based on the fact that the conveyance of the signals required to allow the functioning of web-based services was performed by and within the scope of responsibility of the Internet Access Provider and network operators.[17]

The same logic can essentially be transferred onto Personal Information Management Systems as well. The PIMS provider, through sending, receiving, uploading and forwarding user preferences, personal data and other types of information between the data subject and the data controller, enables a type of communication between those parties. This might even further be extended where both parties possess a user account with the platform. Since these platforms are, however, internet based, the actual conveyance of signals will be performed "wholly or mainly" by the network operators and internet access providers of the respective parties. In conclusion, Personal Information Management Systems should therefore not be considered as electronic communication service providers within the meaning of Art. 2(c) of the Framework Directive. As a result, they will also not be within the scope of the ePrivacy Directive, in accordance with Art. 3 therein.

3. Confidentiality of the Communication

The only Article of the ePrivacy Directive with actual practical relevance for PIMS is Art. 5(3), which concerns the storing of, or the gaining of access to information stored, in the individual's terminal equipment. Art. 5(3) provides that this is only allowed where the user has given his or her consent, based on clear and comprehensive information provided to them. The only exception where consent is not required are instances where this is strictly necessary for the provision of a service explicitly requested by the individual. Typically, this

---

[16]ibid para 37.
[17]ibid para 36.

only covers elements such as cookies needed for allowing the functioning of an online shopping cart or a chatbot.[18] As already explored in Part 1 of this thesis (see Part 1 Chapter 2: D. II. 6. c) bb) (1) Do-Not-Track), there used to be an ongoing legal debate about the relationship between Art. 5(3) of the E-Privacy Directive and the consent requirements enshrined in the GDPR.[19] The fact that GDPR compliant consent is required for the setting of cookies has, however, since then been decided by the CJEU in the *Planet 49* case[20] and largely ended the controversy.[21] It should also be noted that the EDPB has recently adopted Guidelines on the technical scope of Art. 5(3) ePrivacy Directive which provide a detailed overview of the requirements and would therefore need to be considered by providers of PIMS as well.[22]

II. Outlook: the ePrivacy Regulation

While Personal Information Management Systems are not within the scope of the ePrivacy Directive which is currently in force, the future of this legal act including its effect on PIMS should at least briefly be considered. The idea of replacing the currently applicable Directive with a directly binding Regulation has already been in the works for almost a decade.[23] In fact, it was the original intention for

---

[18] *Piltz/Kühner*, 3 ZD 2021, 123, 126f; *DPC*, Guidance on Anonymisation, 6f; *Art. 29 WP*, Opinion 04/2012, 6.

[19] *Haberer*, MMR 2020, 810, 811f; *Rauer/Ettig*, 6 ZD 2015, 255, 257f; *Schmidt/Babilon*, 2 K&R 2016, 86, 86-90; Hoeren/Sieber/Holznagel / *Schmitz*, 'Teil 16.2 Datenschutz im Internet' in Thomas Hoeren, Ulrich Sieber and Bernd Holznagel, HdB MultimediaR, Teil 16.2, para 274-277.

[20] Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 65.

[21] *Rauer/Ettig*, 1 ZD 2021, 18, 18ff; *Spindler*, 35 NJW 2020, 2513, 2513ff; *Böhm/Halim*, 10 MMR 2020, 651, 654.

[22] *EDPB*, Guidelines 2/2023.

[23] *Buttarelli*, 2 EDPL 2017, 155, 155; *Naranjo*, 3 EDPL 2017, 152, 152; *Etteldorf*, 6 EDPL 2020, 567, 567.

the GDPR and the ePrivacy Regulation to come into force simultaneously or at least within a short timeframe from one another.[24] Because of substantial difficulties in reaching an agreement, the project has, however, been stuck in development since then.[25] A substantial source of disagreement are in fact the rules concerning the processing of data stored within the user's terminal equipment, including the usage of cookies,[26] which are quite relevant for PIMS. When and in which form the Regulation will be enacted is still unclear, with some even questioning whether it will in fact become effective at all.[27]

The scope of the Regulation will likely be extended in order to include more modern forms of electronic communication such as messengers, and image and video sharing services, as well as social networks.[28] These types of offerings have been introduced under the term "Over-the-Top communications services" (OTT).[29] This inclusion, however, should have no direct effect on Personal Information Management Systems since these are unlikely to fall within that category.

Potentially of significant relevance are, however, the provisions of Art. 9. Paragraph 1 therein simply confirms what has already been established by CJEU Case Law in the *Planet 49* ruling,[30] namely that the conditions of consent outlined in Art. 4(11) and 7 of the GDPR

---

[24] *Buttarelli*, 2 EDPL 2017, 155, 155; *Naranjo*, 3 EDPL 2017, 152, 152; *Etteldorf*, 6 EDPL 2020, 567, 567; *Gonzalez/de Hert/Papakonstantinou*, in: Data Protection and Privacy, 267, 267.

[25] *Gonzalez/de Hert/Papakonstantinou*, in: Data Protection and Privacy, 267, 267; *Etteldorf*, 6 EDPL 2020, 567, 567; https://www.politico.eu/article/europe-privacy-rules-survived-years-of-negotiations-lobbying/ (accessed: 23 October 2025); Sydow/Marsch / *Sydow*, Art. 95, para 8.

[26] *Etteldorf*, 6 EDPL 2020, 567, 568; https://www.politico.eu/article/europe-privacy-rules-survived-years-of-negotiations-lobbying/ (accessed: 04 March 2026).

[27] *Etteldorf*, 6 EDPL 2020, 567, 573; Sydow/Marsch / *Sydow*, Art. 95, para 8.

[28] Spieker gen. Döhmann/Bretthauer / *Jandt*, E 6.0 Datenschutz im Internet, para 30; Conrad/Auer-Reinsdorff / *Conrad/Hausen*, § 36, para 32.

[29] Spieker gen. Döhmann/Bretthauer / *Jandt*, E 6.0 Datenschutz im Internet, para 30; Conrad/Auer-Reinsdorff / *Conrad/Hausen*, § 36, para 32.

[30] Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801, para 69-75.

also apply for consent collected for the processing of electronic communications data. Art. 9(2) of the draft, however, includes a new clarification that consent for the processing of information stored in and related to end-users' terminal equipment can also *"be expressed by using the appropriate technical settings of a software application enabling access to the internet"*. The idea of allowing consent to be provided by means of browser settings or alternative software solutions, including Personal Information Management Systems, is therefore explicitly being supported.[31] This is in fact quite significant. While the possibility of collecting valid consent by controllers solely through browser settings has not been explicitly excluded before, it has been subject to much debate.[32] After all, the whole legitimacy and admissibility of consent management tools was in fact questioned by many in the context of the regulation on PIMS, found in the new German Telecommunications Digital Services Data Protection Act (TDDDG).[33] The raised concerns are predominantly based on the requirement for consent to be "explicit" and collected separately for each processing activity.[34] The EDPB has attempted to find a middle ground in that regard by stipulating that where browser settings are to be considered, they would need to be sufficiently granular to specify both purposes and individual controllers.[35] Not clear, however, is how the user setting should be treated in the case of a conflict

---

[31]*Botta*, 12 MMR 2021, 946, 949; *Spindler*, 35 NJW 2020, 2513, 2516; *Jones/Lee*, 53 Cornell Int'l L.J. 2020, 97, 122.

[32]Gola/Heckmann / *Schulz*, Art. 7 DSGVO, para 43; *DSK*, *Orientierungshilfe Telemedien,* para 42; *Jones/Lee*, 53 Cornell Int'l L.J. 2020, 97, 118f; *Schermer/Custers/van der Hof*, 16 Ethics Inf Technol 2014, 171, 180.

[33]*Kühling/Sauerborn*, 10 ZD 2022, 531, 532ff; *Kühling/Sauerborn*, 11 ZD 2022, 596, 599; *Botta*, 12 MMR 2021, 946, 948f.

[34]*DSK*, *Orientierungshilfe Telemedien,* para 41ff; *Botta*, 12 MMR 2021, 946, 948; *Jones/Lee*, 53 Cornell Int'l L.J. 2020, 97, 121.

[35]*EDPB*, Guidelines 05/2020, para 89.

between the preferences set up within the browser and those communicated to the PIMS.[36] Based on the principle of privacy by design and default, the more restrictive setting should probably be applied.

III. Interim Conclusions: ePrivacy Directive

The ePrivacy Directive is intended to ensure the protection of privacy in the electronic communication sector. The stipulations of the Directive are supposed to complement and particularise the rules established in the GDPR. Under Article 3 therein, the ePrivacy Directive applies to the processing of personal data related to the provision of publicly available communication services. These are defined as services which are provided for remuneration and are wholly or mainly established for the conveyance of signals on electronic communications networks. PIMS are generally provided for some sort of remuneration and thereby meet the first requirement. They can, however, not be considered as being predominantly concerned with the conveyance of signals.

Functionalities supporting the exercise of data subject rights are likely to provide or exercise editorial controller over the transmitted content, excluding them from the scope. This will in particular apply where the PIMS reviews and requests correction of the answers provided by the controller. Similarly, they might take over or adjust the submissions of the data subject. While consent management functionalities are tasked with communicating the data subjects' preferences and possibly directly transferring the dataset in question, they will not be responsible for the conveyance of the actual signals themselves. These are technically transmitted by the Internet Access Provider, with the PIMS only serving as an intermediary entity between data subject and controller. The obligations put forward by the ePrivacy Directive for providers of electronic communications service will therefore not apply to Personal Information Management Systems.

---

[36] *Kühling/Sauerborn*, 10 ZD 2022, 531, 534ff; *Kühling/Sauerborn*, 11 ZD 2022, 596, 598; Assion / *Aretz*, § 26 TTDSG, para 21-23; *Botta*, 12 MMR 2021, 946, 949f.

The draft of the ePrivacy Regulation, however, includes provisions with a potentially significant effect on Personal Information Management Systems. Art. 9(2) explicitly recognises, the possibility of using technical settings of software applications for the collection of consent. This support of consent management functionalities, managed by other entities than the controllers themselves, is still being heavily debated, making additional clarifications in that regard particularly relevant. Since the Regulation has, however, not yet been adopted with many stipulations still subject to heated debate, it remains to be seen if this provision does in fact make it into the final version. Should the current provision be included, this would certainly be a welcome addition, potentially furthering the development of PIMS, as well as the possibilities of collecting more consumer-friendly consent.

B. Product Liability Directive

The possibility of liability of Personal Information Management Systems under the Council Directive 85/374/EEC, referred to as the Product Liability Directive (PLD), should be considered. While the Directive is not directly applicable, the respective implementations by the Member States will still need to follow the basic rules introduced by such. Furthermore, on 10 October 2024 the council of the EU has adopted a new Directive on liability for defective products (new PLD),[37] which will repeal the current one. The changes brought by the new Directive and their effect on PIMS will therefore also be considered below.

I. Applicability

As outlined in Article 1 of the PLD, the Directive regulates the liability for damages of a producer caused by a defective product.

---

[37]See: European Parliment and Council of the European Union, 'DIRECTIVE (EU) 2024/… OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of … on liability for defective products and repealing Council Directive 85/374/EEC', https://data.consilium.europa.eu/doc/document/PE-7-2024-INIT/en/pdf (accessed: 23 October 2025).

1. Product

It therefore needs to be established whether a Personal Information Management System could even be considered a product under the PLD. Article 2 defines such as *"all movables even if incorporated into another movable or into an immovable"*, including electricity.[38] Since services such as software, applications, or online tools are not "movable" in the traditional sense (although arguably transferable), the question of the extent to which the directive might apply to such has for long been subject to much heated debate among scholars.[39] Differentiations are made based on multiple criteria. Many sources support the idea that where software is part of a machine or other tangible object and is necessary for the functioning of that object, it would be considered movable and thereby constitute a product.[40] Also frequently applied is the differentiation between products and services, which is performed on varying criteria such as the "essence" of the contract[41] or based on whether the software is standardised or custom made.[42] Some sources also attempt to draw an analogy from the explicit inclusion of electricity into the scope.[43]

Considered relevant for a long time was also the differentiation between damages caused by a medium or the information contained in such.[44] While not concerning software but rather print medium, this question has, however, to a large extent been answered by the CJEU in the Case of *Krone*, which dealt with the question if a newspaper

---

[38]Initially primary agricultural products and game where also excluded from the scope, this was however amended by Directive 1999/34/EC as result of the BSE crisis.

[39]*Müller*, Software, 136ff; *Alheit*, 34 CILSA 2001, 188, 188ff; *Fairgrieve/Rajneri*, 1 IWRZ 2019, 24, 24ff; *Schmon*, 6 IWRZ 2018, 254, 255.

[40]*Comandé*, in: European Product Liability, 275, 285; *Alheit*, 34 CILSA 2001, 188, 200; *Triaille*, C.L.S.R. 1993, 214, 218f; *Müller*, Software, 137f.

[41]*Triaille*, C.L.S.R. 1993, 214, 217; *König,* Computerprogramm, 104.

[42]*Müller*, Software, 136; *Alheit*, 34 CILSA 2001, 188, 200 *Comandé*, in: European Product Liability, 275, 285.

[43]*Spindler*, 3 MMR 1998, 119, 120; *Müller*, Software, 108-115.

[44]*Zech*, Information als Schutzgegenstand, 11-15; *Günther*, Produkthaftung, 13f; *Alheit*, 34 CILSA 2001, 188, 200f.

containing incorrect health information could be regarded as a defective product under Article 2 of the PLD.[45] This notion was clearly denied by the CJEU, both with regards to the paper, and the contained advice.[46] The decision has since been criticised and debated for multiple reasons.[47] Most relevant in this context, however, is the fact that if it was consequently applied, it would essentially also prevent the possibility of including software under the scope of the PLD where it is contained in a tangible storage device, previously supported by the prevailing literature.[48]

These controversies and interpretations also apply in determining the nature of PIMS. Since PIMS due to their very broad definition, cannot really be considered a uniform type of offering, there might even be differences in designation for different tools. Most Personal Information Management Systems found on the market are not offered through a movable object but installed in the user's device, either by facilitating local or cloud storage (see Part 1 Chapter 2: A. Storage), potentially excluding them from the scope of the Directive. There is, however, one exception namely the Freedombox home server, which is a server with pre-installed software [49] and which therefore might still be covered. The application of other interpretations does not lead to more uniform results either. When looking at the "essence of the agreement" with various providers, some seem to clearly consider themselves as offering a "service" in the form of

---

[45]Case C-65/20 *Krone* [2021] ECLI:EU:C:2021:471, para 23.

[46]ibid para 43.

[47]See for example: *Mantrov*, 14 EJRR 2023, 416, 416ff; *Twigg-Flesner*, 10 EuCML 2021, 262, 262ff; *Machnikowski*, 30 E.R.P.L 2022, 191, 191f.

[48]*Wagner*, 13 JETL 2022, 191, 200.

[49]FreedomBox, https://freedombox.org/buy/ (last accessed: 23 October 2025).

supporting individuals in understanding and controlling their data-flows.[50] Others, however, market their offerings as "products".[51] The same split between various service offerings would also be present when applying the differentiation between custom made[52] and standardised[53] software, with some PIMS even offering both possibilities.[54]

In conclusion, at the time of writing the applicability of product liability rules to Personal Information Management Systems was both doubtful and inconsistent. It should, however, be noted that the European Commission, being aware of the fact that the current product liability regime does not accurately reflect the realities of the digital economy introduced substantial changes to the existing definition in the new PLD. Article 4 No. 1 of the new PLD defines a product as *"all movables, even if integrated into another movable or into an immovable"* and further specifies that this *"includes electricity, digital manufacturing files, raw materials and software"*. The differentiation between product and service will also no longer be relevant for PIMS since Art. 4 No. 3 of the new PLD also extends the scope to digital services, integrated into a product in a way that its absence would prevent its performance as a *"related service"*. These changes are crucial, especially since the question of including software into the

---

[50]See for example: MyDex, https://mydex.org/ (last accessed: 23 October 2025); PrivacyCheck, https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg (last accessed: 23 October 2025); *Austin and others*, Towards Dynamic Transparency.

[51]See for example: World Data Exchange, https://worlddataexchange.com/features (last accessed: 23 October 2025); CozyCloud, https://cozy.io/en/ (last accessed: 23 October 2025); DataBox, https://databox.com/?origin=20231 (last accessed: 23 October 2025).

[52]Meeco, https://www.meeco.me/powered-by-meeco (last accessed: 23 October 2025).

[53]PrivacyCheck, https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg (last accessed: 23 October 2025); CozyCloud, https://cozy.io/en/ (last accessed: 23 October 2025).

[54] DataBox for example has various standardized dashboards (Client Dashboard, Business Dashboard, Marketing Dashboard, Social Media Dashboard), as well as a "Custom Dashboard". See: DataBox, https://databox.com/?fp_ref=juju34&origin=20231 (last accessed: 23 October 2025).

scope of the PLD has been postulated in academic literature for a long time.[55] It can therefore be assumed that, while at the moment various interpretations might be followed, at least in the near future PIMS will definitely fall under the product liability regime in the EU. The only exception would be, if a PIMS provider supplied an open-source software outside of their commercial activity, as the new PLD does not apply to such (Art. 2(2) new PLD).

2. Producer

Article 3(1) of the PLD defines the producer as *"the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer"*. The consideration of the PIMS provider as a producer can therefore be easily affirmed, since the developers of such transparently lay down their involvement. This is, after all, arguably necessary, as the entire purpose of managing one's data flows through a third party is the separation from the other data controllers by involving an objective entity. The same will be the case under the new Product Liability Directive which introduces the liability of the "manufacturer" rather than "producer" who is defined as *"any natural or legal person who: (a) develops, manufactures or produces a product; (b) has a product designed or manufactured, or who markets that product under its name or trademark or has a product designed or manufactured, or who, by putting their name, trademark or other distinguishing features on that product, presents themselves as its manufacturer; or (c) who develops, manufactures or produces a duct for its own use"* under Art. 4 No. 10.

---

[55] *Wuyts*, 5 JETL 2014, 1, 5-7; *Wagner*, 13 JETL 2022, 191, 200ff; *Comandé*, in: European Product Liability, 275, 285; *Alheit*, 34 CILSA 2001, 188, 199-203.

II. Liability

Under Article 1 of the Product Liability Directive, the producer of a product will be liable for any damages caused by a defect in the offered product.

1. Damages

Article 9 of the PLD defines the types of damages which might be claimed. These are namely damages caused by death or personal injuries and damages to property which are used in the private context and are also intended for such private use. The Directive also specifies that property damage needs to be above 500 European Community Units (ECU), excluding the possibility of claiming smaller losses.[56] While member states may introduce national laws granting liability for non-material damages, these are not part of the PLD.

a) Comparison to the GDPR

This quite restrictive definition stands in stark contrast to the regime of liability under the GDPR. Here Art. 82(1) not only explicitly states the option to claim compensation for both material and non-material damages but Recital 146 furthermore provides that the concept of damages is to be interpreted broadly in a manner which fully reflects the objectives of the GDPR. Especially for the processing of personal data, material damages are rare and significantly harder to assess due to the rather intangible nature of this human right. After all, even the most severe unauthorised data transfers or disclosures are unlikely to result in direct financial losses unless they lead to identity fraud, resulting in an outflow of money or other resources. More relevant are immaterial hardships such as discrimination, loss of confidentiality, or social disadvantages. In such instances, how-

---

[56] *Wuyts*, 5 JETL 2014, 1, 23; *Alheit*, 34 CILSA 2001, 188, 197.

ever, data subjects will not be entitled to any claims against the producer of a Personal Information Management System based on the PLD.

b) In the new PLD

The new draft of the PLD broadens the definition of "damages". First of all, medically recognised harm and psychological health are included into the scope of personal injuries (Art. 6(1)(a) new PLD). Also, the heavily criticised 500 ECU deductible has been removed.[57] This extension is quite relevant for the potential liability of PIMS, as negative psychological effects are more likely to occur in the context of the right to privacy, compared to direct financial losses. The change between only covering property used or consumed privately to only excluding *"property used exclusively for professional purposes"* (Art. 6(1)(b)(iii) new PLD) is, however, of no practical relevance in this context since PIMS naturally only concern the processing of the individual's personal (and thereby inherently private) data.

Most importantly, however, Art. 6(1)(c) new PLD also established *"destruction or corruption of data that are not used for professional purposes"* as a completely new type of damages. This inclusion is intended to accurately portray the changes in our digital economy, where data in itself has become a commercially viable good.[58] As a result, essentially all types of data processed via a Personal Information Management System will be within the scope of the Directive, as PIMS per definition are intended to protect the individual's personal data, not business information. The protection for damages caused by Personal Information Management Systems will therefore essentially become equally broad under the new PLD, as it currently is for damages caused by data controllers under the GDPR.

---

[57] *Wagner*, 13 JETL 2022, 191, 209; *Fairgrieve/Howells*, 50 MLR 2007, 962, 974f; *de Meeus*, 4 EuCML 2019, 149, 151.

[58] *Wagner*, 13 JETL 2022, 191, 211; *Ritter/Mayer*, 17 DLTR 2017, 220, 220; *Hacker*, 2 ZfPW 2019 148, 148ff.

2. Defectivness

In order for the producer to be liable for the established damages, the product which caused such would also need to be defective. Under Article 6 of the PLD, a product is defective where it does not provide the level of safety which an individual is entitled to expect under the given circumstances. This includes the presentation of such a product (Art. 6(1)(a) PLD), the use to which the product can reasonably be expected to be put (Art. 6(1)(b) PLD), and the time at which the product was put into circulation (Art. 6(1)(c) PLD). Article 6(2) PLD goes on the specify that solely the fact that a higher quality product was put into circulation at a later time cannot be considered a defect.

This reliance on the consumer's perspective, also referred to as the "consumer expectation test", has been subject to much criticism within literature based on its general vagueness, as well as the fear that unreasonable expectations of consumers would result in an increase in damages.[59] In general, the types of defects can be divided into (1) manufacturing defects, which occur when the product deviates from the specifications set out by the respective producer; (2) design defects, determined based on the general industry customs and standards, as well as economic factors, and (3) instruction defects, also referred to as "failure to warn", which consider the necessity and adequacy of warnings in light of the producer's knowledge regarding certain dangers.[60] Heavily debated in that context is, however, whether the consumer expectation test allows for the inclusion of a risk-benefit-analysis, by which the risks posed by a product would be weighed against its benefits or whether a risk-utility-analysis should be deployed, requiring the producer to avoid risks at all costs.[61] At least the German Federal Court of Justice has supported

---

[59] *Luzak*, 11 EJRR 2020, 630, 631; *Veldt*, 1 EuCML 2023, 24, 26; *Alheit*, 34 CILSA 2001, 188, 196; *Wagner*, 13 JETL 2022, 191, 204; *Fairgrieve/Howells*, 50 MLR 2007, 962, 967.

[60] *Fairgrieve*, 4 EuCML 2019, 170, 171; *Alheit*, 34 CILSA 2001, 188, 196.

[61] *Veldt*, 1 EuCML 2023, 24, 26; *Wagner*, 13 JETL 2022, 191, 204; *Luzak*, 11 EJRR 2020, 630, 646.

the notion of considering a risk-utility-test as a relevant criterion in a case dealing with the liability of a manufacturer for the faulty triggering of an airbag.[62]

a) Potential Defects of the PIMS

In Personal Information Management Systems, the established defect would likely have to relate to the processing of an individual's personal data. The two principal components on which PIMS market themselves can be summarised as "safety" and "control". Safety in the sense of securely storing personal data and keeping unwanted parties from accessing it[63] and control in the sense of both gaining a better understanding of one's dataflows,[64] and managing consent and other types of access modalities.[65] Based on these definitions, potential defects might include (1) a failure to appropriately secure the data from outside attacks; (2) data transfers not in line with the preferences set up by the data subject; (3) a failure to retrieve data from another controllers; (4) a failure to delete information, where requested by the individual; or (5) unwanted disclosures of personal data. Also imaginable is the occurrence of instruction defects, for example in the form of unclear or incorrect privacy notices or a lack of warning given to the data subject before agreeing to high-risk processing activities.

---

[62]BGH, NJW 2009, 2952, para 18.

[63]See for example: CozyCloud, https://cozy.io/en/ (last accessed: 23 October 2025); Nextcloud, https://nextcloud.com/de/ (last accessed: 23 October 2025); MyDex, https://mydex.org/ (last accessed: 23 October 2025); Meeco, https://www.meeco.me/ (last accessed: 23 October 2025).

[64]See for example: PrivacyCheck, https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg (last accessed: 23 October 2025); Polisis, https://chrome.google.com/webstore/detail/polisis/bkddolgokpghlbhhkflbbhhjghjdojck (last accessed: 23 October 2025); Meeco, https://www.meeco.me/ (last accessed: 23 October 2025).

[65]See for example: Advanced Data Protection Control, https://www.dataprotectioncontrol.org/ (last accessed: 23 October 2025); MyDex, https://mydex.org/ (last accessed: 23 October 2025); Meeco, https://www.meeco.me/ (last accessed: 23 October 2025).

Especially for data security, it is necessary to determine what level of safety would be considered as "reasonable to be expected" by the data subject. As has already been outlined while establishing what types of security measures would be regarded as "appropriate" under Art. 32(2) of the GDPR in PIMS (see Part 1 Chapter 2: A. III. 1. Appropriateness), the baseline should be significantly higher for Personal Information Management Systems. This is because, unlike with other businesses where the processing of personal data is only a side-effect to the primary activities, the main purpose of a PIMS lies in the support of the data subject realising their rights. The data subject, or in the case of product liability, the injured person can therefore reasonably expect that the product will be state-of-the-art in ensuring data security.

This assumption might, however, cause some friction with Art. 6(2) PLD, which excludes liability solely based on the fact that a better product is put into circulation at a later stage. Here, the question might arise at what point the provider would be required to update their security standards if the industry standard changes. Minor differences in forms of encryption, transfer, or storage might not automatically trigger a requirement on the side of the PIMS to change their product. If such a tool was to be marketed as ensuring the highest levels of security, however, changes in the state-of-the-art would need to be considered as an individual should be assumed to have a "reasonable expectation" that the promised level of security would be kept up to date, considering changes on the market.

It should also be noted that under the current liability regime, such an obligation to update one's product based on the state-of-the art would only affect tools sold or put into circulation after the change in industry standards but not those which have been previously purchased. The reason for this is that Art. 7 PLD uses the moment of putting a product into circulation as the relevant threshold by which its defectiveness should be measured. Art. 7(b) PLD excludes liability where a defect did not exist at that time or came into being afterwards, whereas Art. 7(e) PLD clarifies that the same applies where the state of the scientific and technical knowledge at that time would not have allowed for the defect to be discovered. This limitation of

liability is based on the notion that once a product is put on the market, it has left the sphere of influence of the producer.[66]

b) In the new PLD

This assumption, however, does not hold true for most digital products such as software and online platforms since in most instances, the producer will still have access to these even after the initial sale.[67] Here it is common practice for businesses to offer upgrades, patches, and other types of modifications, both by conducting such remotely or requesting the user to install a new version.[68] This has been taken into account by the European Commission in the newly proposed draft of the Product Liability Directive. Article 7(1)(e) new PLD clearly separates instances under which the manufacturer retains control after putting a product onto the market in listing the moment in which the product has *"left the control of the manufacturer"* as a relevant element when assessing the defectiveness of the product. Furthermore, *"safety-relevant cybersecurity requirements"* are also explicitly mentioned in Article 7(1)(f) new PLD. The same notion is also further supported in the exemptions listed under Article 11(2) DPLD. Here the exemption from liability under 11(1)(c) DPLD is explicitly excluded where the defectiveness of the products is based on a related service, a software (including updates and upgrades), or the lack of updates and upgrades which are within the manufacturer's control.

The newly proposed Product Liability Directive therefore expressly includes a requirement for software and other digital products to be updated in line with the existing industry standards, as long as the manufacturer still can access such or exercise control over them. The obligations of such manufacturers to provide security updates

---

[66] Case C-127/04 *O'Byrne* [2006] ECLI:EU:C:2006:93, para 27 ff, *Borghetti*, in: European Product Liability, 205, 217; *Schmon*, 6 IWRZ 2018, 254, 257.

[67] *Hacker*, CLSR 2013, 105871, 28; *Hacker*, AI Regulation in Europe, 17; *Wagner*, 13 JETL 2022, 191, 206; *Veldt*, 1 EuCML 2023, 24, 26.

[68] *Hacker*, CLSR 2013, 105871, 28; *Hacker*, AI Regulation in Europe, 17; *Wagner*, 13 JETL 2022, 191, 206; *Veldt*, 1 EuCML 2023, 24, 26.

are further laid down in the newly proposed Cyber Resilience Act (CRA).[69] The connection between those two acts, has been explicitly recognised in Recital 16 CRA. Annex I of the Act, listing essential security requirements, establishes the obligation to *"ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users"* (Annex I 1. (3) (k) CRA) and to *"provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner"* (Annex I. 2. (7) CRA) for all manufacturers of products with digital elements (Art. 10(1) CRA). This requirement will directly affect providers of Personal Information Management Systems, as those are predominantly offered as digital platforms, in which the provider has constant control over the content. Even where the data is locally stored on the users' device and the provision of regular updates, it can be expected that the producer ensures a high level of security.

3. Causation

Once the existence of damages and a defect in the product has been affirmed, a causal relationship between the two needs to be established. This is quite relevant since in practice many claims for damages are in fact rejected by courts, based on the failure to establish a causal link between the two.[70] This is also not without relevance for PIMS, especially considering that even while the tool might still be "within the manufacturer's control", most decisions regarding the actions taken by such will be made by the data subject itself.

---

[69] *European Commission,* Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

[70] *European Commission*, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products, 28f; *Schmon*, 6 IWRZ 2018, 254, 258.

Where the individual provides their final approval for a certain action, it might therefore be hard to establish a direct link between the damages and the defect. For example, should certain facts concerning the processing of personal data by a potential controller to which data might be transferred be misrepresented to the individual and a decision to allow such a transfer be based on that, the manufacturer could still argue that the causal link between the damages caused by that transfer lies in the individual's agreement and not the misrepresentation. The same problem might apply with breaches of security caused by external attacks. Here it could be questionable whether it was in fact a defect or rather the attack which caused the damages and if such could have even been prevented by additional security measures.

4. Burden of Proof

The problem in establishing a causal link between the defect and the damages is particularly relevant since the burden of proof under the product liability directive lies on the side of the injured party, in accordance with Art. 4 PLD. The specifics of the procedure, the form in which evidence is gathered, what is admissible etc. is left to the Member States to be specified in national law. However, national courts will still be required to interpret these provisions in line with the PLD, excluding the possibility of introducing any legal presumptions or rules for reversing the burden of proof.[71] This puts a great deal of responsibility on the consumer.

a) In the Context of PIMS

This can be considered quite burdensome, especially when considering that the injured individual will often not even have direct ac-

---

[71] *Schmon*, 6 IWRZ 2018, 254, 257f; *de Meeus*, 4 EuCML 2019, 149, 152; *Wuyts*, 5 JETL 2014, 1, 23f.

cess to information concerning the technical specifications and functioning of certain products.[72] Even where access to such details is granted, they may often lack the knowledge and expertise to accurately assess both the defectiveness and the existence of a causal link between a product and the damage.[73] While Member States have developed certain ways to support the consumer in proving their claim such as, for example, placing obligations to disclose information on producers or ordering joint payment for expert fees,[74] the burden of proof still constitutes a significant burden for the injured individual. This problem will be particularly evident with damages caused by Personal Information Management Systems. After all, here the data subject will often opt for the use of such tools precisely because they feel overwhelmed and misinformed while making decisions regarding the processing of their personal data. The reason for involving a PIMS therefore lies specifically in the self-identified lack of expertise and understanding of the subject. The result under which they would now be required to gain such expertise in order to prove the causality therefore seems particularly unfair.

b) In the new PLD

The new PLD provides for some rules which are intended to mitigate this inequality between the parties and support the injured individual in making their claim where necessary. Art. 9(1) new PLD postulates that national courts should have the power to order the disclosure of information relevant for the case where a claimant has presented evidence and facts which make their claim for compensation plausible. Also, while Art. 10(1) new PLD still puts the general burden of proof for the existence of damages, a defect, and a causal link on the claimant, it further introduces several relevant presumptions to support the injured party.

---

[72] *Schmon*, 6 IWRZ 2018, 254, 258; *de Meeus*, 4 EuCML 2019, 149, 152; *Wuyts*, 5 JETL 2014, 1, 24.

[73] *Fradera*, 26 E.R.P.L. 2018, 707, 710; *de Meeus*, 4 EuCML 2019, 149, 152; *Wuyts*, 5 JETL 2014, 1, 24.

[74] *Wuyts*, 5 JETL 2014, 1, 24.

Defectiveness is presumed under Art. 10(2) new PLD where (a) the defendant did not comply with the obligation of disclosure under Art. 9(1) new PLD; (b) the product does not comply with mandatory safety requirements based on Union or national law; or (c) an obvious malfunction occurred, which caused the damage during normal use. The presumption for obvious malfunctions might, for example, help the data subject where their personal data was wrongly disclosed to third parties, either based on a defect in the consent management or a lack of security measures. After all, such disclosures, regardless of their reason would clearly indicate an improper functioning of the platform occurring during normal use. The presumption of Art. 19(2)(b) new PLD might become quite relevant, where Member States decide to enact laws governing the requirements for such tools. As already established above, this is, for example, the case in § 26 of the German TDDDG, which obliges the Federal Government to create rules governing the functioning and requirements for consent management tools. Similarly, the Data Governance Act, which will be analysed in more detail herein (see Part 3 Chapter 6: D. Data Governance Act), sets out numerous obligations for so called "data intermediation services".

Based on Art. 10(3) new PLD, the causal link between the defect and the damage can be presumed if the defectiveness of the product has been established and the damages which occurred are *"of a kind typically consistent with the defect in question"*. This again simplifies matters tremendously for the data subject, since as long as there is a likely connection between damage and defect, they will not have to explicitly prove how exactly the defect led to the unwanted outcome. Furthermore, Article 10(4) new PLD provides that where, based on technical and scientific complexity, the claimant faces "excessive" difficulties in proving either the defectiveness or the causal link, both can be presumed if the product at least contributed to the damage and it is likely that it was defective or that the defect caused the damage. This leads to a significant relaxation of the standard of proof, since essentially it only needs to be established that considering the circumstances, the causation of damage by the manufacturer

was likely.[75] What is unclear is the question at which point the difficulties encountered by the individual would be considered "excessive".[76] Recital 48 new PLD provides some clarification, referring to "*technical or scientific complexity*" in particular and providing some practical examples of such scenarios. In the context of PIMS the complex nature of the technology used could apply as a factor. Recital 48 new PLD also explicitly mentions machine learning as an example. It should also be noted, that since PIMS users will often decide to use an intermediary specifically because they require support in managing their data, their level of expertise also be presumed as being quite low. Still courts will need to make a determination on a case-by-case basis, looking at the type of difficulties as well as the position of the particular claimant and the manufacturer.

III. Interim Conclusions: Product Liability Directive

When assessing the potential liability of the PIMS provider under the European Product Liability regime, the qualification of such as a "product" would first need to be determined. This, however, is at least questionable under the current Directive, which does not accurately reflect the market realities for digital services. Also, differences between various platforms have led to a largely inconsistent interpretation based on various theories. This issue, however, has been solved under the new PLD adopted on 10 October 2024, which explicitly includes software as well as related services, into the scope of the Directive. The role of a producer (or manufacturer) can also easily be affirmed for the PIMS provider.

For the types of damages which may be claimed, it should be noted that the PLD provides for a quite restricted definition, including only damages caused by death or personal injuries and damages to property, which was used in the private context and was also intended for such private use. This stands in stark contrast to the very broad interpretation explicitly postulated by the GDPR. There are,

---

[75] *Wagner*, 13 JETL 2022, 191, 218.

[76] ELI, COM Prop. for a Rev. PLD, 19; *Veldt*, 1 EuCML 2023, 24, 30.

however, again some changes in that regard since the new PLD significantly broadens the current definition by including medically recognised harm and psychological health into the scope of personal injuries, as well as establishing loss or corruption of data as a new type of damage. Based on that, all types of data processed though PIMS would automatically be included within the scope, in effect equating the term in the new PLD and the GDPR.

In order to determine whether a specific product is defective, the consumer expectation test is typically applied. For PIMS it should be assumed that consumers may have a higher expectation level for the security of their data as this constitutes the primary component of the tool. Providers of PIMS would, however, technically not be required to update or upgrade their product as the current Directive still judges the defectiveness based on the moment at which the product was put onto the market. This will change under the new PLD which shifts that baseline to the point at which a product left the control of the manufacturer, meaning that owners of platforms and tools will be required to upgrade and update their product as long as they can exercise control over such.

What might be quite problematic for data subjects is that the burden of proving damages, defectiveness, and causation lies on their side. This can be considered extremely difficult where the individual lacks proper insight into the functioning of the platform or simply technical knowledge in order to gain such an understanding. The new PLD does, however, provide for a number of presumptions which significantly ease this inequality between the parties, further supporting the individual user.

While the current Product Liability Directive therefore does not add to the protection of PIMS users in any relevant manner, the substantial changes introduced in the new PLD have a lot of potential. Since the GDPR only allows for damages to be claimed from the data controller or processor (Art. 82 GDPR), compensation under the new PLD might be a viable alternative for individuals, where the PIMS is not qualified as one of those. Also positive in that regard is the inclusion of psychological health into the scope of personal injuries (Art. 6(1)(a) new PLD). Slightly problematic might be the reference in Recital 24 new PLD, which states that privacy infringements *"should not*

by themselves trigger liability under this Directive". It can however be presumed, that this only applies to instances where no other damage, in the form of psychological harm resulted from the infringement.

C. Data Governance Act

In June 2022, Regulation (EU) 2022/868 of the European Parliament and of the Council of May 30, 2022 on European data governance and amending Regulation (EU) 2018/1724, also referred to as the "Data Governance Act" (DGA), came into force.[77] It is part of the new European Data Strategy and should support the creation of an inclusive data driven economy for all EU citizens (Recital 2 DGA). The EU intends to establish European data spaces, covering areas such as *"health, mobility, manufacturing, financial services, energy or agriculture, or a combination of such"*, so that data can be findable, accessible, interoperable, and re-usable, under the "FAIR data principle" (Recital 2 DGA). This, covers not only personal data in the meaning of the GDPR, but under Art. 2 No. 1 DGA *"any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording"*. Most relevant, however, for Personal Information Management Systems is the introduction of rules governing the functioning of so called "Data Intermediation Services" in Chapter III of the DGA.

I. Data Intermediation Services

The definition of data intermediation services can be found in Art. 2 No. 11 of the Data Governance Act, where they are defined as *"a service which aims to establish commercial relationships for the pur-*

---

[77] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152.

poses of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data".

1. Relevant Parties

The definition of data intermediation services in the DGA introduces three types of parties (additionally to the service itself), namely the data subject, the data holder, and the data user.

a) Data Subject and Data Holder

Art. 2 No. 7 DGA clearly sets out that the term "data subject" has the same meaning as it does in Art. 4 No. 1 of the GDPR. The term "data holder" however, is new. Under Art. 2 No. 8 of the DGA it means any natural or legal person which is not the data subject but based on applicable law may grant access to, or share certain types of data (personal or not).

Article 10 DGA sets out a clear differentiation between data intermediation services between data holders and data users (Art. 10(a)) and between data subjects and data users (Art. 10(b)). This would suggest that one person could not take both roles at the same time. Legal entities naturally cannot take the role of a data subject but those are also not relevant in the context of PIMS, which based on the definition applied at the heart of this thesis are limited to tools offered directly to the data subject. PIMS are clearly intended to fall under the type of data intermediation services established in Art. 10(b). The assumption, however, that this would automatically exclude them from taking the role of a data holder, cannot be followed. As has been established while discussing the term "personal data", the same information can be personal data of multiple individuals, for example, if it clearly relates to a specific person but information about another individual might also be drawn from it (see Part 2 Chapter 3: A. II. 4. b) Relating to). Such instances are also not uncommon. Information about the savings, owned real estate, or income of an individual will naturally also indirectly affect and relate to the financial status of their spouse and children. Health data will also often allow

for conclusions to be drawn about the future well-being of one's offspring. Another textbook example might be pictures of friends and family. They naturally make up personal data of the platform user, who either might be in those pictures or additionally save some memories of loved ones. The data relates to that person, making them the data subject. However, the same pictures will also be personal data of all the other individuals present in those images. Excluding the possibility of managing such "multi-relational" data would essentially be impossible, since most information has the potential of relating to multiple individuals.[78] It would therefore need to be included in the scope, as long as it is also related to the data subject.[79] Here, however, other individuals will also be data subjects without being users of the PIMS. The upload of photos or other data to personal data storage is not prohibited by the GDPR, as it falls under the household exemption of Art. 2(2)(c) GDPR but it still constitutes processing of personal data of other individuals. The PIMS user will therefore, while still being a data subject, also take on the role of a data holder under the DGA as they are processing the personal data of other individuals while having the legal right to do so.

While Art. 10(b) also includes types of services between data users and natural persons that seek to make non-personal data available, this is of little relevance for PIMS, since those are per definition designed to facilitate the handling of personal data. It is also arguably hard to imagine what type of data would be non-personal when it comes to data shared by a natural person, since arguably, any type of information shared through such a platform would relate to them.

b) Data User

The term data user is defined under Art. 2 No. 9 as the natural or legal person who is lawfully accessing data and has the right to further use such. With Personal Information Management Systems, this will therefore be the data recipient processing data through the PIMS.

---

[78]Specht-Riemenschneider/Hennemann / *Specht-Riemenschneider*, Art. 10 DGA, para 35.

[79]ibid para 35.

The DGA does not introduce any restrictions regarding who can take that role.[80] It should be examined whether for PIMS, the term "data user" would always automatically be equated with the position of "data controller" under the GDPR. Based strictly on the definitions at hand, this would be likely. Both include natural and legal persons within their scope. A controller would need to determine the means and purposes of the processing under Art. 4 No. 7 GDPR. Since Art. 2 No. 9 DGA mentions the data users right to *"use that data for commercial or non-commercial purposes"*, this could be understood as naturally resulting in the determination of such. On the other hand, a processor who is processing data on behalf of a controller could also be understood as using it for commercial purposes and having the right to do so, based on the data processing agreement.

Another indicator could be the reference to having "lawful access" in the definition of "data user" under the DGA. At a first glance, this might be associated with the principle of lawfulness and therefore the presence of a legal basis under Art. 6 of the GDPR in the case of accessing personal data, supporting the correlation between data controllers and data users. Again, however, data processors are also processing personal data lawfully on behalf of others based on Art. 28 GDPR. In that sense, while in practice data users accessing personal information through a data intermediation service will probably be classified as data controllers as well, the two terms cannot be considered equal and instances under which data processors might be considered data users acting on behalf of another controller are at least imaginable.

2. Purpose

Additionally, to setting out the types of parties involved in data intermediation services, Art. 2 No. 11 also outlines the purposes for which they are to be used. The principal aim of data intermediation services is the facilitation of data sharing between an undetermined number of actors.[81] Art. 10(b) also similarly mentions the purpose of

---

[80] ibid para 39.

[81] *Schweitzer and others*, Data access and sharing, 278.

making personal data available. The term data sharing has been defined in Art. 2 No. 10 as *"the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge"*.

a) Consent

What comes first to mind in this regard are typical consent management functionalities, discussed under Part 1 Chapter 2: C. Consent. This would fall under the category of "voluntary agreement", being that consent is per definition freely given. The DGA also expressly recognises and supports the definition of consent established in the GDPR in Art. 2 No. 5. Likewise, data transfers based on performance of contract (Art. 6(1)(b) GDPR) could also be considered as a form of voluntary agreement of the individual. Based on the reference to the provision based on Union or national law, the legal basis under Art. 6(1)(c) GDPR (compliance with a legal obligation), could also serve as the basis for such a transfer.

Questionable, however, is to what extent data transfers based on Art. 6(1)(d), (e) and (f) would still be within the scope of the DGA, even if conducted through an intermediary. Data transfers for the protection of vital interests are at first rare but will generally occur where the data subject cannot consent and tend to pertain to circumstances involving an element of time-pressure.[82] Making data accessible via a data intermediation service in such life-and-death situations is therefore extremely unlikely. The problem with the legal basis of Art. 6(1)(e) GDPR, which refers to the necessity for the performance of tasks carried out in the public interest or in the exercise of an official authority, is that in principle it can only be used by public

---

[82]Ehmann/Selmayr / *Heberlein*, Art. 6, para 32; Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 51-54; *Schantz* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 6 Abs. 1, para 62.

authorities.[83] Art. 2 No. 11(d), however, clearly excludes data sharing services offered by legal entities within the public sector which do not aim at establishing a commercial relationship from the scope. While public sector bodies are not excluded from taking the role of data user, they would need to receive the data in the context of a "commercial relationship" which is not possible for the legal basis of Art. 6(1)(e) GDPR.[84] As for the legal basis of legitimate interest under Art. 6(1)(f), none of these restrictions applies, as it is typically used by a business for processing activities furthering their commercial interests.[85] On the other hand, it will probably be applied where consent cannot be obtained from the data subject, either because of a lack of means to contact such or due to their lack of agreement with the processing in question.[86] Such data transfers are therefore again unlikely to occur via intermediation services which explicitly require the establishment of a relationship between the data subject or a data holder and the data user.

b) Requests

Functionalities supporting the exercise of a data subject request also seem to be directly included within the scope of Art. 10(b), which explicitly mentions intermediation services *"enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679*". The provision of services supporting the individual in acting on their rights is enshrined in Article 15–20 of the GDPR, namely the rights to access, rectification, erasure, restriction of processing, and portability, as discussed in Part 1 Chapter 2: D. Request is therefore included

---

[83]Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 54; Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 25.

[84]Ehmann/Selmayr / *Heberlein*, Art. 6, para 34-37; Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 61; Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 23.

[85]Ehmann/Selmayr / *Heberlein*, Art. 6, para 40f; Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 28.

[86]Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 26; *Schantz* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 6 Abs. 1, para 88-92.

within this scope.[87] This is also supported by Recital 30 of the DGA, which explicitly mentions all of those rights. As a result, the scope of data intermediation services is widened from just facilitating the sharing or making available of data. Some of these rights are, after all, specifically directed at the opposite by means of regaining or completely removing information from the data user. They can, however, still be viewed as supporting the underlying purpose of these types of services, as they ultimately are parts of navigating the envisaged (commercial) relationship between the parties.[88]

Interestingly, the right to object is not referenced in Recital 30 DGA, raising the question if service offerings supporting the exercise of such would not be included within the scope. This assumption would in a sense be supported by the finding of the previous considerations on the legal basis for processing under Art. 6(1) GDPR, which might apply to data intermediation services. It has been established that the applicability of Art. 6(1)(e) and (f) is unlikely to occur. In the first instance, based on the aim of creating a "commercial relationship", as this would go against the requirement of necessity for tasks carried out in the public interest or in the exercise of an official authority. [89] In the second instance, because the legal basis of legitimate interest will typically be used, where there is little no direct contact with the data subject, which should not be the case for data intermediation services. [90] As the right to object, however, only applies to those two legal bases (Art. 21(1) GDPR), PIMS functionalities supporting such are likely to fall outside of the scope of Art. 10(b).

Should therefore a Personal Information Management System be aimed at supporting all or multiple data subject rights, scenarios might occur under which part of the service offering might be subject to the requirements of the Data Governance Act and part not. Such

---

[87]Specht-Riemenschneider/Hennemann / *Specht-Riemenschneider*, Art. 10 DGA, para 40.

[88]*von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 275.

[89]Ehmann/Selmayr / *Heberlein*, Art. 6, para 34-37; Gola/Heckmann / *Schulz*, Art. 6 DSGVO, para 57; Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 23.

[90]Paal/Pauly / *Frenzel*, Art. 6 DSGVO, para 26; *Schantz* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 6 Abs. 1, para 88-92.

an artificial "splitting" of a consolidated platform is, however, neither in the interest of the data subject, nor could it have been in the intention of the lawmakers. Based on that, since Art. 10(b) does not exclude any data subject rights and Recital 30 only refers to such which are included *"in particular",* an extended interpretation should be supported under which functionalities supporting the exercise of the right to object should also be within the scope of Art. 10(b) DGA where the overall service offering would be considered a data intermediation service under the Data Governance Act.[91]

c) Transparency

A similar dilemma occurs in transparency enhancing technologies discussed under Part 1 Chapter 2: B. Information, as the right to information is again not mentioned in Recital 30 of the DGA. Additionally, Recital 28 states that where a service provider offers multiple data-related services, only those directly concerning the assurance of data intermediation should be covered by the Act. On the other hand, the Recital does set out that the services in question could include *"advising individuals on the possible uses of their data and making due diligence checks on data users before allowing them to contact data subjects, in order to avoid Fraudulent practices"*. This could in a sense be understood as an obligation to include transparency enhancing mechanisms within the service offering. After all, the previously analysed interpretative functionalities (see Part 1 Chapter 2: B. III. 1. Interpretative) do in a sense constitute a form of advice, especially when elements such as an evaluation of the controller's privacy practices or furthermore recommendations on alternative providers are included. Similarly, the reviewed auditing tools (see Part 1 Chapter 2: B. III. 2. Auditing), could be understood as a form of *"due diligence check*", especially when reviewing the controllers' actual processing practices against statements made in their privacy policy. The overall intent of transparency enhancing technologies is

---

[91] *von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 275.

also consistent with the general purpose of data intermediation services, as these are intended to navigate the relationship between the data recipient and the data subject, by enabling the individual to select parties with which they would like to engage. The support of the right to information should therefore also be considered within the scope of Art. 10(b), where it is part of a platform intended to facilitate the sharing of data.[92]

There is, however, some uncertainty on how to treat platforms such as Polisis[93] or the Usable Privacy Project[94] which analyse privacy policies without facilitating any further establishment of a relationship between the data controller and the data subject.[95] The notion of the data intermediation service, taking the leading role in forging a direct connection between data subjects (or data holders) and data users, seems to lie at the heart of the Data Governance Act.[96] This is again supported by Recital 28, which explicitly excludes services which only provide technical tools for data sharing but *"neither aims to establish a commercial relationship between data holders and data users nor allows the data intermediation services provider to acquire information on the establishment of commercial relationships for the purposes of data sharing"*. Transparency enhancing technologies, solely aimed at interpreting or auditing a controller's privacy practices without facilitating a direct relationship between the parties will therefore probably fall outside of the scope of the Data Governance Act.

d) Storage

The same type of differentiation will probably apply to data storage related functionalities, analysed in Part 1 Chapter 2: A. Storage. Recital 28 DGA, after all, even explicitly denies cloud storage services,

---

[92] Specht-Riemenschneider/Hennemann / *Specht-Riemenschneider*, Art. 10 DGA, para 40.

[93] *Harkous and others*, USENIX 2018, 531, 531ff.

[94] *Sadeh and others*, Usable Privacy Policy Project.

[95] *Schweitzer and others*, Data access and sharing, 285.

[96] ibid 280.

which solely provide the technical tools for data sharing but do not aim to establish a commercial relationship between data subjects and users, the characterisation as a data intermediation service. Where a platform does serve the purpose of facilitating the data transfer between two actors, storage functionalities within the PIMS would, however, still fall within the scope of Art. 10(b) DGA. After all, Art. 10(b) established that the offering of a data intermediation service also includes *"making available the technical or other means to enable such services"*. Including additional functionalities is also recognized in Art. 12(e), which specifies that specific tools and services serving the purpose of facilitating data exchanges such as, for example, temporary storage may be included. Furthermore, Recital 30 also recognises the possibility of storing personal data with the intermediary, by asserting that *"it could be desirable to collate actual data within a personal data space so that processing can happen within that space without personal data being transmitted to third parties in order to maximise the protection of personal data and privacy"*. While therefore pure storage solutions (whether locally or within the cloud) would not be within the scope of the Data Governance Act, Personal Information Management Systems through which the individual manages their data and storage functionalities would definitely be included.[97]

II. Consequences

Since it has been established earlier in this thesis that in fact most service offerings of Personal Information Management Systems would fall under the scope of data intermediation services under the Data Governance Act, the question of the legal consequences resulting from such a designation needs to be posed.

---

[97] Specht-Riemenschneider/Hennemann / *Specht-Riemenschneider*, Art. 10 DGA, para 40; *Schweitzer and others*, Data access and sharing, 281.

1. Conditions

Article 12 of the DGA sets out a substantial number of conditions for the provision of data intermediation services. First, similar to § 26(1) No. 2 of the German TDDDG, it establishes them as a type of neutral entity which may not use the data in question for any purposes outside of the intermediation itself (Art. 12(a) DGA).[98] Furthermore, personal data generated about the user as a part of such service can also only be used for its further development (Art. 12(c) DGA). The intermediation service is additionally in a sense tasked with protecting the data subject, as Art. 12(f) asks for the assurance that the access to data is fair, transparent, and non-discriminatory. Art. 12(g) stipulates the prevention of fraudulent or abusive practices. Art. 12(m) also sets out a requirement to *"act in the data subjects' best interest where it facilitates the exercise of their rights"*.

There are also several analogies with the rights and freedoms provided for under the GDPR. Article 12(o) DGA, for example, introduces a type of accountability requirement by obliging data intermediation services to maintain a log record of their activities. Art. 12(d) DGA can be considered as supporting the right to data portability, since it requires service providers to ensure the exchange of data in the format selected by the data subject, while allowing the conversion into other formats for enhancing its interoperability across sectors.[99] The general goal of supporting interoperability is furthermore underlined in Art. 12(i) DGA. Also analogous to the obligation of implementing appropriate technical and organisational measures in order to secure personal data established in Art. 32 of the GDPR, Art. 12(j) and (l) DGA ask that adequate *"technical, legal and organisational measures*" are put in place to prevent unauthorised access or transfers and that *"necessary measures"* are taken for the assurance of an appropriate level of security for the storage, processing and transmission of data. Interestingly, however, Art. 12(k) only requires intermediation service providers to inform data holders of the occurrence

---

[98] *von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 282.

[99] *Kühling*, 45 DuD 2021, 783, 787; *von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 283.

of unauthorised transfers, access, or use of non-personal data. It should therefore be assumed that where such events concern personal data, the general regime of notifying the supervisory authority and the data subject, established in Articles 33 and 34 of the GDPR, shall apply.

2. Notification

Besides the conditions for the provision of data intermediation services set out in Art. 12, the Data Governance Act also establishes a regime of control by requiring the notification of such to the competent authority (Art. 11(1) DGA). The type of information which should be included in such is outlined in Art. 11(6) DGA and essentially covers only basic contact details and an indication of the type of intermediation services which are to be provided. After the submission of this notification, the service provider can in principle start the activity with no further review or confirmation from the authority (Art. 11 (4) DGA).[100] It is, however, possible to request both a declaration confirming the submission of the notification (Art. 11(8) DGA), as well as the compliance with the requirements set out in Art. 12 DGA (Art. 11(9) DGA). In the second instance, providers will even be allowed to use the label "data intermediation services provider recognised in the Union", for which a logo will be developed.

3. Monitoring

Once an intermediation service has been notified, the competent supervisory authorities (which should have been designated by all Member States by September 24, 2023, based on Art. 13(1) DGA) are tasked with monitoring the compliance of these service providers with the requirements set out in the Act (Art. 14(1) DGA). For this purpose, they are given several powers such as (1) requesting all the information necessary to verify such compliance (Art. 14(2) DGA); (2) notifying the provider of any identified deficiencies and giving

---

[100] *von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 281.

them the opportunity to state their views (Art. 14(3) DGA); (3) requiring the cessation of any infringements within a reasonable timeframe (Art. 14(4) DGA); (4) imposing financial penalties (Art. 14(4)(a) DGA); (5) requiring postponement of the commencement or a suspension of the service (Art. 14(4)(b) DGA); or (6) requiring the cessation of the service (Art. 14(4)(c) DGA).

4. Liability

It is important to note that the Data Governance Act, while setting up conditions for the provision of data intermediation services as well as introducing a regime of monitoring their compliance with such by the competent supervisory authorities, is essentially silent on the question of liability for any type of damages caused by these tools.[101] The term "liability" is in fact only mentioned in Recital 33 of the DGA, which states that questions of liability for any detriment, material, or immaterial damages caused by the actions of the service provider may be addressed within the contract between the parties based on national liability regimes. This is in a sense surprising, considering the otherwise quite comprehensive regime regulating such services introduced by the Act. In consequence, data subjects cannot bring forward any claims for damages based directly on the Act but will rather need to carefully review the terms of services put forward by the provider.

5. Complaint

Individuals are also left with no means of forcing the provider into compliance with the Act. While Art. 14(1) DGA establishes that the competent authorities may monitor and supervise compliance *"on the basis of a request by a natural or legal person"*, this does not introduce a requirement for the authority to act based on such complaints.[102] Based on this, individual data subjects are essentially left

---

[101] *Schweitzer and others*, Data access and sharing, 289.

[102] Specht-Riemenschneider/Hennemann / *Specht-Riemenschneider*, Art. 10 DGA, para 32.

with no effective forms of acting against such a data intermediary. This stands in stark contrast to how complaints by data subjects are handled in data protection law. Here, where a complaint has been issued under Art. 77(1) GDPR, Art. 78(2) essentially introduces a legal requirement for the supervisory authority to handle such and inform the individuals of its progress, giving them a right to an effective judicial remedy against the supervisory authority should they fail to do so. This legal requirement of the supervisory authorities to handle requests and issue decisions based on such, has in fact already been confirmed by Member States Courts, for example by the Stockholm Administrative Court, in the Case No. 13308-22.[103] The possibility of issuing a complaint based on privacy regulations can, however, not be considered as an appropriate alternative since complaints under Art. 77 of the GDPR can only relate to infringements of the Regulation and not any other laws.

6. Effect on the Roles taken by the GDPR

Additionally, to directly establishing rules governing the relationship between data intermediation services, data subjects, data holders and data users, the regulations found in the Data Governance Act may also affect the roles taken by those tools under the GDPR. As has been discussed under Part 1 Chapter 3: A. II. 1. a) bb) Implicit Legal Responsibility previously, one of the bases from which controllership can be derived is implicit legal designation. This will be the case where the legal provision establishes a task or a responsibility which cannot be fulfilled without processing personal data and where the entity fulfilling that task is designated as responsible for such processing.[104] The provisions of the DGA include several indications as to the roles taken by such tools under the GDPR.

---

[103] Förvaltningsrätten i Stockholms, DOM 2022-10-31, Meddelad i Stockholm, Mål nr 13308-22.

[104] *EDPB*, Guidelines 07/2020, para 22; *Voigt/von dem Bussche*, GDPR, 19; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 14.

First, Recital 35 determines that *"[w]here the data intermediation services providers are data controllers or processors as defined in Regulation (EU) 2016/679 they are bound by the rules of that Regulation"*. It thereby clearly supports the notion that intermediation services could take on both roles and that there is no pre-established designation. In order to subsume providers under one of the terms, Art. 12 of the DGA is likely to be the most indicative. As has already been established, Art. 12(a) excludes the use of data by the provider for any other purpose than the provision of the service itself and Art. 12(c) only allows for data generated about the user as a part of such service to be used for its further development. The Article therefore explicitly establishes the purposes of processing for the data intermediation service, leaving open the determination of the means. It introduces a clear differentiation between the intermediation services and the data users. The means and purposes of processing for the intermediation itself and the further development of the platform lie solely on the side of the data intermediation service provider, making them the data controller for such. For any other processing activities which result from the intermediation, the service provider is legally prohibited from having any interest or determining the purposes, automatically excluding them from taking such a role and effectively making the data user the controller.

The scope of controllership of data intermediation services is, however, not as limited as it might appear at first glance. Art. 12(e) DGA, for example, provides that the services may also be provided for purposes such as facilitating the exchange of data, temporary storage, curation, conversion, anonymisation, and pseudonymisation. This means that these actions will therefore again fall within the scope of "providing the service" and the area within which the intermediation service provider is determining the means and purposes of processing personal data, taking the role of data controller under Art. 4 No. 7 GDPR. The same will also apply for the storing of activity logs, required by Art. 12(o) DGA, and the conversion of data to different formats to ensure interoperability (Art. 12(d) DGA).

Particularly interesting are the instances under which the intermediation service might take the role of a processor. These seem slightly problematic, since the DGA clearly intends to set them up as

an independent and impartial mediator. This is evident in Art. 12(f), which asks for providers to ensure that the access to their service be *"fair, transparent and non-discriminatory for both data subjects and data holders, as well as data users"*. The role of processor, however, as per definition would ask for processing to be conducted *"on behalf of"* one of the parties, including the fact that the processor will be bound by the instructions of the controller (Art. 29 GDPR). This might lead to a conflict of interest, especially if the intermediation service were to assume the roles of a processor in relation to the data user. Article 12(m) also creates the requirement of acting in the data subjects' best interest, where it facilitates the exercise of their rights. If, therefore, the interests of the data user and data subject do not align, the service would be excluded from concluding a data processing agreement. More likely to occur are instances where the service provider takes the role of a data processor in relation to the data holder, who has their own right of sharing and granting access to data (Art. 2 No. 8 DGA).

Also, relevant when considering the interplay between the DGA and the GDPR is the question to what extent the first might be considered a *lex specialis* to the latter. After all, both the European Data Protection Supervisor and the European Data Protection Board have voiced their concerns with regard to certain provisions of the DGA, stating that the need to ensure the protection of personal data has not been sufficiently accounted for.[105] Should the DGA therefore be considered *a lex specialis* for data intermediation services and by extension PIMS, there might have been a risk of circumventing certain guarantees provided in the GDPR.[106] The Opinion of the EDPB and EDPS was, however, based on the initial proposal published on November 25, 2020.[107] Since then, significant changes have been made to the document, most notably the inclusion of Art. 1(3), which explicitly specifies that the DGA is without prejudice to GDPR (and other privacy relevant regulations) and that in the event of a conflict,

---

[105] *EDPB/EDPS*, Joint Opinion 03/2021, para 18-21.
[106] *Vardanyan/Kocharyan*, 9 Eur. Stud. 2022, 91, 99.
[107] *EDPB/EDPS*, Joint Opinion 03/2021, para 8.

law on the protection of personal data shall prevail. In that sense, even though the DGA with its specific rules for data intermediation services might be considered a *lex specialis* for Personal Information Management Systems, this would have no effect on the applicability of the requirements of the GDPR.

III. Interim Conclusions: Data Governance Act

The Data Governance Act which came into force in June 2022, introduces several rules governing the functioning of so called "data intermediation services". These are defined as services aiming *"to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data"*. While the main purpose of Personal Information Management Systems lies in the support of the data subject in the enforcement of their rights, they are still likely to fall under that definition.[108]

Although consent management functionalities will without a doubt be covered by the term, constituting a form of "voluntary agreement", data transfers based on performance of contract (Art. 6(1)(b) GDPR) or compliance with a legal obligation (Art. 6(1)(c) GDPR) are also imaginable. Functionalities supporting the exercising of data subject requests are also directly included within the scope of Art. 10(b) DGA as it mentions intermediation services *"enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679"*. With Transparency Enhancing Technologies, a differentiation needs to be made between services solely focused on the analysis of privacy policies without the facilitation of actual data transfers and such which, as part of their overall service offering, including the establishment of a relationship between data subjects and data users, also offer

---

[108] *Botta*, 12 MMR 2021, 946, 949; *Richter*, 3 ZEuP 2021, 634, 650; *von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 275; *Schwartmann/Hanloser/Weiß*, PIMS im TTDSG, 3.

mechanisms for transparency enhancement. While the first are unlikely to be considered data intermediation services under the DGA, the latter should be assumed to fall under the Regulation. A similar distinction can be made for Personal Information Management Systems providing storage functionalities. Here as well, pure storage solutions would not be included within the scope of the Data Governance Act, while PIMS, through which the individual manages their data in general including storage functionalities as part of the overall service offering, would definitely fall under the term.[109]

As a result, Personal Information Management Systems which are also covered by the term "data intermediation services", will be subject to the notification procedures put forward in Art. 11 of the DGA, as well as required to meet the conditions for such services established in Art. 12 DGA. The Data Governance Act, however, does not introduce a specific regime of liability for such services, referring to the contract between the parties and national legislation instead. The possibilities for individuals to issue complaints against such services are also severely limited. While Art. 14(1) allows the competent authorities to monitor and supervise compliance based on an individual request, it does not create any obligation to follow up on these complaints or other grievances.

The regulations established in the DGA may affect the roles taken by data intermediation services under the GDPR. Based on the conditions set forward in Article 12 DGA, it can be assumed that the service provider will take on the role of controller for all data processing related to the intermediation itself, as well as any additional services such as storage, curation, conversion, anonymisation, and pseudonymisation. They might also take the roles of a processor, as long as they can still act impartially, as well as in the data subject's best interest. Based on that, they are more likely to take that role with regards to data holders rather than users, although the latter may still be possible.

---

[109]Specht-Riemenschneider/Hennemann / *Specht-Riemenschneider*, Art. 10 DGA, para 40.

D. Data Act

Another part of the new European "Data Strategy" is the Regulation on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, also referred to as the "Data Act" (DA), which came into force on January 11, 2024.[110] The regulations found therein cover multiple areas and are quite extensive. First, Chapters II and III establish rules under which users of connected devices or other parties may access data generated by these tools.[111] Chapter IV attempts to protect small and medium enterprises from unfair contractual terms related to data access and use.[112] Chapter V lays down rules on making data available to public sector bodies.[113] Finally, Chapter VI intends to support customers in their options to easily switch between data processing services.[114]

I. Applicability

Considering the broad scope of the Regulation, there are several areas that are potentially relevant for providers of Personal Information Management Systems. One cornerstone of the Data Act is the notion that the sharing of data should be encouraged and promoted in order to ensure fair competition, as well as to avoid lock-in-

---

[110]Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance) [2023] OJ L, 2023/2854.

[111]*Schreiber*, 8 MMR 2023, 541, 541; *Carovano/Finck*, 50 CLSR 2023, 105830, 14; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 812; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 51.

[112]*Podszun/Pfeifer*, 13 GRUR 953, 955; *Schreiber*, 8 MMR 2023, 541, 541; *Carovano/Finck*, 50 CLSR 2023, 105830, 14; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 812.

[113]*Carovano/Finck*, 50 CLSR 2023, 105830, 14; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 812 *Podszun/Pfeifer*, 13 GRUR 953, 955; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 51.

[114]*Schreiber*, 8 MMR 2023, 541, 541; *Carovano/Finck*, 50 CLSR 2023, 105830, 14; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 812.

effects.[115] The specific obligations related to that are, however, varying for a number of different parties.[116] The extent of applicability to PIMS should therefore be examined separately.

1. Connected Products and Related Services

Article 3 establishes rules for the design, manufacturing, and provision of connected products and related services, all of which are defined by Art. 2 No. 5 and 6 respectively. As far as feasible, product and related service data should be directly accessible to the user and by default, provided easily, securely and free of charge in a comprehensive, structured, commonly used, and machine-readable format. In that sense, a type of requirement for "data accessibility by design and default" is created.[117]The term "connected product" refers to items which obtain, generate, or collect data concerning their environment and can communicate this information. The primary target group includes smart home appliances, smart cars, connected health care monitors, and connected security systems.[118] Here the fear is that providers of such devices have a potentially unfair advantage based on the vast amounts of data available to them.[119] While the specification that a product shall be "physical" has been removed from Recital 14, the term "item" still likely requires some sort of physical presence or the ability to move an object.[120] After all, digital services and software related to a product would need to be

---

[115]*Metzger/Schweitzer*, 1 ZEuP 2023, 42, 47; *Podszun/Pfeifer*, 13 GRUR 953, 953; *Richter*, 3 MMR 2023, 163, 163; *Wiebe*, 4 GRUR 2023, 227, 227; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 809.

[116]*Metzger/Schweitzer*, 1 ZEuP 2023, 42, 51.

[117]*Steinrötter*, 4 GRUR 2023, 216, 220; *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 52; *Schreiber*, 8 MMR 2023, 541, 542; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 815; *Podszun/Pfeifer*, 13 GRUR 953, 956; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 52.

[118]*Assion/Willecke*, 11 MMR 2023, 805, 806; *Podszun/Pfeifer*, 13 GRUR 953, 953; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 814.

[119]*Richter*, 3 MMR 2023, 163, 163.

[120]*Specht-Riemenschneider*, 5 ZRP 2022, 137, 138; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 814.

considered as related services under Art. 2 No. 6.[121] Most PIMS service offerings are provided purely online and would thereby likely be excluded.[122]

The only currently available PIMS which has a physical presence other than "on-device" storage is the Freedombox home server, which contains pre-installed software.[123] Both this form, as well as any on-device storage, would have been excluded from the scope based on Recital 15.[124] The content of this has, however, substantially changed compared to the initially introduced draft.[125] The new Recital 15 seems to now incorporate an almost limitless amount of data points into the scope, including intentionally and unintentionally generated data, data relating to activity, as well as inactivity and even information collected from sensors. Still from a logical standpoint, a PIMS would on its own not fall within this scope. While the system might generate metadata in the sense of user access to an application, set-up preferences, and data transfers, this data is not really being communicated with other services in any form and is in a sense "generated" by the user themself. Where personal data or a consent signal is transferred, this information is not really "collected" by the device but rather channelled through it since the action is initialised directly by the user and the result obtained by the data controller. It is likely that future Personal Information Management Systems could communicate with smart devices, for example, based on the user's request by collecting data from a connected product and forwarding it in accordance to the data subject's preferences. This, however, would not cause the PIMS to become a "connected" product themselves but rather one mode of electronic communication or as discussed under the next point, a data holder.

A PIMS will also not be considered a "related service" in the meaning of Art. 2 No. 6. Such services would need to be connected with

---

[121] *Specht-Riemenschneider*, 5 ZRP 2022, 137, 138.

[122] *Specht-Riemenschneider*, 5 ZRP 2022, 137, 138.

[123] FreedomBox, https://freedombox.org/buy/ (accessed: 23 October 2025).

[124] *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 51; *Specht-Riemenschneider*, 5 ZRP 2022, 137, 138.

[125] *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 814.

the product in such a way that the absence of such a connection would prevent the performance of certain functionalities.[126] Personal Information Management Systems should, however, per design, not be related or bound to any specific controller but facilitate the connection and transfer of data for any devices or services selected by the user. PIMS will therefore not be subject to the requirements set out in Art. 3 of the Data Act (DA).[127]

2. Data Holders

Further outlined within Chapter II are the rights and obligations of so called "data holders" regarding the access, use, and availability of product and related services data (Art. 4 DA). Data holders are defined under Art. 2 No. 13 of the DA as *"a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service"*.[128] This definition has also notably changed throughout the legislative process.[129]

Still the intention of the lawmakers primarily lies in including parties who may be in possession of the relevant data point into the scope of obliged entities.[130] This may be of particular relevance

---

[126] *Specht-Riemenschneider*, 5 ZRP 2022, 137, 138.

[127] *Carovano/Finck*, 50 CLSR 2023, 105830, 14ff: does not even consider this possibility, while analyzing the effect of the Data Act on data intermediaries.

[128] It should be noted in that context that this definition substantially differs from the one provided in the Data Governance Act, as Art. 2 No. 8 therein defined a data holder as any natural or legal person, which is not the data subject but based on applicable law has the right to grant access to, or share certain types of data (personal or not).

[129] *Carovano/Finck*, 50 CLSR 2023, 105830, 15f.

[130] *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 813; *Carovano/Finck*, 50 CLSR 2023, 105830, 15.

where such a party may have the technical means to block the access to such information.[131] Based on that, the access to data by the user will be ensured, even when individuals cannot get it directly from the connected product or related service (Art. 4(1) DA). It is, however, important to note that the role of a data holder is not to be equated with an actual property right, as any type of control might warrant the designation as data holder.[132]

a) User is the Data Subject

Theoretically, a Personal Information Management System could fall under this definition.[133] It should, however, be noted that they will be excluded from the scope in the context of services provided by them as data processors (Recital 22 DA).[134] Furthermore, the actual practical relevance seems quite limited. It is not only imaginable but also highly likely that a PIMS would retrieve and store data from a connected device of a data subject. This might either happen directly, if consent for the data processing of a connected product was managed through the platform, or indirectly, if, for example, a portability request was submitted to the provider of such products or related services. In turn, they would technically become a data holder. The reason why there is, however, little practical relevance related to that fact is that logically the user (data subject) will already have access to that data via the PIMS. This is, after all, the entire purpose of the platform: to retrieve and manage data on behalf of the individual. Also, where the user and the data subject are the same person, an almost identical claim could be made based on the right to data portability established in Art. 20 GDPR.[135] In that sense, Art. 4(1) DA does not really create a new legal responsibility here, but reiterates

---

[131] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 54; *Carovano/Finck*, 50 CLSR 2023, 105830, 15; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 813.

[132] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 54; *Wiebe*, 4 GRUR 2023, 227, 228.

[133] *Carovano/Finck*, 50 CLSR 2023, 105830, 15.

[134] *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 813.

[135] *Richter*, 3 MMR 2023, 163, 165; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 58.

an already existent relation. The same can be said about the other stipulations of Article 4. The fact that the exercise of the user's rights should not be hindered (Art. 4(4) DA) and that the verification of the user's identity should not require data collection beyond what is necessary (Art. 4(5) DA) naturally results from the purpose of the PIMS and therefore does not require legal specification. Similarly, the obligation enshrined in Art. 5(1) DA. Here the holder is obliged to transfer data to third parties at the request of the user. Again, this is already the whole point of a PIMS: to manage data transfers. Clearly the Data Act also regulates the use and access of non-personal data.[136] Since, however, the entire purpose of PIMS is the management of personal information, it lies in the nature of the service that data held with such a tool would be personal.[137]

b) User is not the Data Subject

More practical relevance might arise for instances where the user and the data subject are separate entities.[138] A user under the Data Act is any natural or legal person who owns a connected product, has the right to use such a product, or receives a related service (Art. 2 No. 12 DA). Considering how much data is being captured by smart devices, it is also conceivable that they will also collect data of other individuals, whether by accident or on purpose.[139] If a person other that the owner drove a smart car, asked the smart fridge if the milk was out, or requested the washing machine to automatically turn on at 6.00 pm, their personal data in the form of driving style, preferred beverages, or estimated time of arrival at home will also be captured.

---

[136] *Steinrötter*, 4 GRUR 2023, 216, 219; *Richter*, 3 MMR 2023, 163, 164.

[137] *Richter*, 3 MMR 2023, 163, 164: refers to a similar logic in the context of IoT devices, based on the notion that those are likely to be attributed to a natural person.

[138] *Steinrötter*, 4 GRUR 2023, 216, 220; *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 76; *Richter*, 3 MMR 2023, 163, 165; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 810; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 56.

[139] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 76; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 56.

This individual might have their PIMS retrieve that data. For example, a roommate who moves out no longer wants this information stored on their friend's device. As a result, based on Art. 4(12) DA, the owner of the device might request access data generated by the connected product about their roommate or other inhabitants from the PIMS. Similarly, they may have that information transferred to third parties based on Art. 5(7) DA.

The user would, however, need to have a legal basis in accordance with Art. 6 or 9 of the GDPR.[140] In the imagined roommate scenario, anything other than consent is unlikely to apply. Should the user, on the other hand, be a legal entity such as, for example, an employer or service provider of the data subject, legitimate interest (Art.6(1)(f) GDPR) or the applicability of a legal obligation (Art.6(1)l GDPR) are imaginable.[141] For example, a company using a connected car might be interested in accessing information about the frequency of use or covered distances. Also possible would be the applicability of Art. 6(1)(e) GDPR where the user is a public agency.[142] In requests to access data based on legitimate interest, it has been suggested that the data holder (here the PIMS) might be required to take certain technical measures such as anonymisation or aggregation in order to ensure that the principles of data minimisation and purpose limitation are being adhered to.[143] While such access to data via a PIMS would therefore be theoretically imaginable, it should still be noted that it is highly unlikely. Users interested in these types of data-points from their connected devices will probably be provided with much easier access directly through the product, a related service, or other types of data holders, especially since the PIMS would naturally only have the data of their specific user available. The same will also apply in the case of potential access by

---

[140] *Steinrötter*, 4 GRUR 2023, 216, 220; *Richter*, 3 MMR 2023, 163, 165; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 811.

[141] *Steinrötter*, 4 GRUR 2023, 216, 220; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 810.

[142] *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 810.

[143] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 78; *Hartmann/McGuire/Schulte-Nölke*, 2 RDi 2023, 49, 58.

public sector bodies, outlined in Chapter V.[144] Should, however, a product user deem this form of access as preferable, the Personal Information Management System will be obliged to grant such without undue delay, free of charge, continuously and in real-time in accordance with the Regulation.[145]

3. Data Processing Services

While the practical relevance of PIMS as data holders seem quite limited, the extent to which they might take on the role of a data processing service should also be examined. The term is defined in Art. 4 No. 8 DA and refers to any digital service which *"enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction"*. This definition is purposefully broad as confirmed by Recital 81, which specified that the term covers a large amount of services with varying purposes, functionalities, and technical set-ups. The Recital also explicitly mentions Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models, as typical examples. Personal Information Management Systems are therefore likely to fall within this scope, especially where they include storage or data transfer functionalities.[146] As a result, the PIMS provider will need to ensure compliance with the obligations laid down in Chapters VI, VII and VIII of the Data Act.

a) Switching

Chapter VI establishes an obligation for data processing services to enable the switching between different providers covering the same service type (Art. 23). This means that Personal Information

---

[144] *Richter*, 3 MMR 2023, 163, 167.

[145] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 55; *Carovano/Finck*, 50 CLSR 2023, 105830, 15.

[146] *Carovano/Finck*, 50 CLSR 2023, 105830, 16.

Management Systems will need to ensure that data subjects are free and able to select a different PIMS provider and that there should be minimal practical hurdles to making such a change.[147] While the competitiveness of a specific PIMS might be challenged by this, the overall state on the market is likely to improve as any type of lock-in strategies will be prevented.[148] This right of the customer should be explicitly outlined in a written contract between the parties, the specific terms of which are established in Art. 25. The PIMS will also need to ensure that the data subject is aware of this possibility by providing relevant information on available switching procedures (Art. 26(a) DA), as well as a reference to an online register which provides details of all the data structures, data formats, relevant standards, and open interoperability specifications (Art. 26(b) DA). The PIMS website will also need to transparently communicate the jurisdiction to which their ICT infrastructure is subject and include a generalised description of the measures taken in order to prevent informational governmental access or transfer of non-personal data (Art. 28 DA). Furthermore, after a three year transitional period, charging the individual for the provision of support in switching services will be banned (Art. 29(1) DA).

b) Access Prevention

Article 32 of the Data Act stipulates that providers of data processing services are required to take adequate technical, organisational and legal measures to prevent international and third-country governmental access to or transfer of non-personal data. This stipulation is likely of little Practical relevance in Personal Information Management Systems, who will predominantly process personal data. Additionally, it has already been established that PIMS providers would already be subject to high security requirements (see Part 1 Chapter 2: A. III. 1. Appropriateness).

---

[147] *Hennemann/Steinrötter*, 21 NJW 2022 1481, 1485; *Podszun/Pfeifer*, 13 GRUR 953, 958; *Carovano/Finck*, 50 CLSR 2023, 105830, 16.

[148] *Schreiber*, 8 MMR 2023, 541, 542; *Carovano/Finck*, 50 CLSR 2023, 105830, 16.

c) Interoperability

The interoperability between different systems should be ensured in order to allow individuals the use of multiple service providers at the same time (Art. 34(1) DA). This means that the different components of the tool need to be able to exchange and use data in order to perform their functions (Art. 2 No. 40 DA). Here again the possibility for data subjects to freely choose between varying providers is significantly strengthened as potential hurdles for data transfers are effectively removed.[149] What is, however, not entirely clear is to what extent a service provider would also need to ensure that the other service can function properly with the offered exchange formats.[150]

II. Enforcement

Article 37(1) DA provides that the Member States should designate one or more competent authority which will be responsible for the application and enforcement of the Act. However, the respective national supervisory authorities established under Art. 51 GDPR will monitor compliance with the Data Act where personal data is concerned (Art. 37(3) DA). PIMS are therefore still primarily likely to interact with the respective data protection authorities since the data processed by them will, by design, be personal. Art 37(5) provides several powers for the competent authorities, such as (a) promoting data literacy and awareness; (b) handling complaints; (c) conducting investigations; and (d) imposing financial penalties, as well as initiation proceedings for the imposition of fines. The Data Act does not provide for any maximum amount but lists the business's annual turnover of the preceding financial year as one factor which should be considered when making a determination (Art. 40(3)(f) DA). Data Protection Authorities may, however, refer to the criteria as well as amounts established in Art. 83 of the GDPR when imposing fines for violations of Chapters II, III and V (Art. 40(4) DA).

---

[149] *Carovano/Finck*, 50 CLSR 2023, 105830, 16; *Schreiber*, 8 MMR 2023, 541, 542; *Podszun/Pfeifer*, 13 GRUR 953, 958f.

[150] *Heinzke*, 6 GRUR-Prax 2023, 154, 156.

While the idea of private enforcement is largely left out of the Regulation, claims based on breach of contract where the conditions outlined within the Act are not complied with, are likely to occur.[151] Not clear, however, is to what extent claims to grant data access could be brought directly before Member States Courts.[152] This lack of focus on private enforcement is in a sense surprising when considering how much emphasis is put on the contractual relationship between the different parties in the Data Act.[153] In the case of PIMS, the data subject will still have the option to claim damages based on Art. 82 of the GDPR. In fact, there has been a constant rise of civil procedures concerning compensations for violations of the GDPR over the years.[154] Claims under Art. 82 GDPR can only be made against controllers and processors. However, even if the Data Act has granted a similar right, this would not make a difference to the data subject since the DA seems to equate the data holder with the controller (Recital 22 DA).

III. Extended Effect

Despite the above discussed requirements to which Personal Information Management Systems may also be subject, the new Data Act might in fact have an even broader effect on such technologies. While the roles of intermediaries or data intermediation services are not specified,[155] they are referenced in Recital 33. It is stated here that both data intermediation services, as defined under the Data Governance Act, and Personal Information Management Systems could support users in the establishment of commercial relations with

---

[151] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 79; *Wiebe*, 4 GRUR 2023, 227, 237; *Podszun/Pfeifer*, 13 GRUR 953, 960.

[152] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 79; *Wiebe*, 4 GRUR 2023, 227, 237.

[153] *Podszun/Pfeifer*, 13 GRUR 953, 960.

[154] *Leibold*, 5 ZD-Aktuell 2022, 01092; *Paal/Kritzer*, 34 NJW 2022, 2433, 2433-2438; *Wybitul/Leibold*, 4 ZD 2022, 207, 207-215; *Paal*, 51 NJW 2022, 3673, 3673ff.

[155] *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 79f; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 819; *Lühmann/Schumacher/Stegemann*, 3 ZD 2023, 131, 131-136.

their potential counterparties in the context of the purposes outlined by the Data Act. Furthermore, they are described as potentially playing *"an instrumental role in aggregating access to data so that big data analyses or machine learning can be facilitated, provided that users remain in full control of whether to provide their data to such aggregation and the commercial terms under which their data are to be used"*. This essentially evidences that, while technically some of the obligations enshrined in the Data Act might apply to PIMS, they are certainly not the primarily intended addressees. Quite the opposite: they are rather seen as a type of entity which may support individuals in managing their relationship with providers of connected and related services, data holders, and data processing services. This makes sense since the general goal of the Data Act—to promote better and fairer access to information and thereby support innovation—[156] is a notion shared by supporters of PIMS as well. The rules and obligations established with the Data Act might therefore potentially support the further development of Personal Information Management Systems, as it has created many new potentials for intervention by such.[157]

IV. Effect on Roles taken under the GDPR

The Data Act clearly recognises the fact that there are multiple overlaps with the GDPR as personal data will also fall within the scope of "data" under Art. 2 No. 1 DA. In that regard, it provides under Art. 1(5) that it is without prejudice to both national and EU law concerning the protection of personal data and that in the event of a conflict between the Data Act and the GDPR (or national law adopted based on such), the laws regarding the protection of personal data or privacy shall prevail. This means that where obligations under the

---

[156] *Hennemann/Steinrötter*, 21 NJW 2022 1481, 1482; *Metzger/Schweitzer*, 1 ZEuP 2023, 42, 47; *Podszun/Pfeifer*, 13 GRUR 953, 953 *Richter*, 3 MMR 2023, 163, 163; *Wiebe*, 4 GRUR 2023, 227, 227; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 809; *Heinzke*, 6 GRUR-Prax 2023, 154, 154.

[157] *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 819; *Carovano/Finck*, 50 CLSR 2023, 105830, 14.

DA would lead a PIMS provider to potentially violate rules under the GDPR, the latter should always take preference.

While the regulations of the Data Act do not make any specifications as to the roles taken by providers of connected products and services, users, data holders or data processing services under the GDPR, they are in fact mentioned on multiple occasions within the Recitals. First and foremost, Recital 22 excludes processors from being data holders. While they may be tasked to make data available by the controller, they shall not have any direct obligation under the Data Act. This seems quite logical, since based on Art. 28(1) GDPR they should only carry out processing operations (including data transfers) on behalf of the controller and based on their instructions. In PIMS, however, this could lead to potentially problematic results. As has been established in Part 2 of this thesis (see Part 2 Chapter 4: E. Findings for Part 2), PIMS may technically take any of the roles defined under the GDPR (or even none) depending of the specifics of the respective service offering. For example, data transfers in the context of ensuring the right to portability or to receive a copy might be performed solely as a processor;[158] similarly, in exercising the right to restriction.[159] In fact, for certain features PIMS might even not take any role, as is, for example, the case with certain transparency enhancing technologies.[160]

In functionalities performed by the PIMS as a processor, this means that they will not be required or even more so allowed, to act on any user requests under the Data Act. As a result, a PIMS provider might have an obligation to provide access to data under Chapter II of the DA for certain datasets managed by them but not for others, leading to a potentially confusing result for all parties. This again evidences how crucial a consistent and coherent designation of roles for PIMS is, supporting the here presented view that PIMS

---

[158]See Part 2 Chapter 4: D. II. 1. c) aa) Security of the Copy or D. II. 5. b) bb) Transmission.

[159]See Part 2 Chapter 4: D. II. 4. Restriction.

[160]See Part 2 Chapter 4: B. I. 1. Standardised Translations and II. 1. Standardised Audits.

should uniformly take the role of data controller. Furthermore, the Data Act does not clarify whether entities with no role under the GDPR could qualify as data holders. It can, however, be assumed that if processors are excluded from the scope, the same should apply to third parties.

Whereas the fragmentation of roles within Personal Information Management Systems is seen critically in this thesis, the practical consequences in the context of the applicability of the Data Act might not be quite as drastic. As has been established previously (see Part 3 Chapter 6: D. I. 2. Data Holders), PIMS are in general unlikely to have much relevance as data holders, based on simple impracticability. Should a request for access under Chapter II of the DA be directed against a PIMS, this will probably relate to data physically stored by them. While PIMS take various roles in service offerings relating to transparency or data transfers, it has been concluded under Part 3 Chapter 6: A. III. Interim Conclusions: Storage that they should generally be considered as data controllers in the context of storage related functionalities. This minimises the potential for fragmentation. It is, however, important to note that while this was the conclusion reached from the conducted legal analysis, it does not reflect market realities where in fact many PIMS present themselves as processors or even third-party intermediaries, considering the users (therefore either the data subject or data recipient) the controller.[161] As a result, these service providers will probably not be willing to comply with the Data Act as well. This again evidences the importance of designating Personal Information Management Systems as controllers.

Another specification concerning the roles of the user can be found in Recital 34. The Recital confirms that the roles of user and data subject are not to be equated with one another and establishes that personal data may only be requested by data controllers or data subjects. Potential scenarios in that regard have already been discussed under Part 3 Chapter 6: D. I. 2. b) User is not the Data Subject. The assumption that the user would need to either be a data

---

[161] See Part 2 Chapter 4: A. II. 3. Current Practice.

subject or a controller can also essentially be derived from the stipulations of Art. 4(12) and Art. 5(7) DA, which clarify that where the user is not the data subject, any request for personal data would require a legal basis for processing in accordance with Art. 6 or 9 of the GDPR.[162] Since a legal basis for processing is a general indicator for controllership, [163] this would therefore be the only sensible conclusion. Recital 34 furthermore considers the possibility for the data user and the data controller to be considered as joint controllers in certain circumstances. In PIMS, this will most likely be the case where a specific functionality requires active communication and agreement on certain technical questions between the platform and the controller. [164]

Not mentioned, however, are any type of restrictions for the categorisation as data processing services. It can therefore be assumed that these might take any role under the GDPR. This is also quite logical since offerings such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) models will in fact typically be considered as processors in accordance with Art. 28 GDPR.[165]

V. Interim Conclusions: Data Act

The Data Act is also part of the EU's overall Data Strategy and is intended to support free access to data in order to further data driven value creation and ensure a fair and competitive market which would benefit society as a whole. This is done through a number of regulations setting out rules for accessing data generated by connected

---

[162] *Steinrötter*, 4 GRUR 2023, 216, 220; *Richter*, 3 MMR 2023, 163, 165; *Specht-Riemenschneider*, MMR-Beilage 2022, 809, 811.

[163] *DSK,* Kurzpapier Nr. 13, 2; *EDPB*, Guidelines 07/2020, para 167.

[164] See Part 2 Chapter 4: D. I. 2. b) bb) Independent Platforms or D. II. 2. a) Rectification at the Source and b) Creation of Link.

[165] *DSK,* Kurzpapier Nr. 13, 4; *CNIL*, GDPR, 2; Sydow/Marsch / *Ingold*, Art. 28, para 18-23.

products, as well as enabling free switching between service providers. While Personal Information Management Systems will not qualify as connected or related products under the Act, they may be considered data holders, should data from such products be stored or managed through their platforms. In that context, they may receive requests for access to data from both the data subjects subscribed to their platform but also other parties who are users of the connected product in question. This option, however, seems purely theoretical at the moment, as other data holders will probably possess more comprehensive datasets not limited to one natural person. More importantly, however, Personal Information Management Systems will be considered data processing services under Art. 4 No. 8 DA. Based on that, they will be required to enable individuals to freely switch between different providers covering the same service type (Art. 23) and ensure interoperability between different systems for the purposes of in-parallel use of different services (Art. 34(1) DA).

While the Data Act considers the establishment of new competent authorities for its enforcement, the national data protection authorities are still responsible where personal data is concerned. PIMS will therefore likely still only be required to interact with those. While several powers are assigned to the authorities, the possibility of private enforcement is rarely mentioned within the Act making it likely that damages of individual users would still primarily be claimed based on Art. 82 of the GDPR.

Additionally, to PIMS being subject to certain obligations under the Data Act, there is also a more general, extended effect of the new law for these types of services. Based on Recital 33, it can be assumed that the lawmakers consider PIMS and other data intermediation services as entities which may support individuals in managing their relationship with providers of connected and related services, data holders, and data processing services. PIMS are viewed as supporting the goals of the new data strategy, and the new obligations of businesses under the Data Act might create even more opportunities for their development.

The Data Act also provides some specifications as to the roles taken by data holders and users under the GDPR. While these are not found directly in the Articles but solely in the Recitals, they still

provide relevant insight. Based on this, data holders should always be controllers, whereas a user could be both a controller and a data subject. Processors and third parties are therefore excluded from the scope of those two terms. They may, however, still be considered data processing services since the DA makes no specification in that regard.

E. Digital Services Act

Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19, 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC, also known as the Digital Services Act came into force on November 16, 2022. These intend to support the creation of a safe digital space in which the fundamental rights of users are protected (Art. 1(1) DSA) by laying down harmonised rules governing the provision of intermediary services (Art. 1(2) DSA). This traces back to the fact that the Commission considered the previous E-Commerce Directive as largely "outdated", since in particular issues such as hate speech and fake news were not addressed therein.[166] The notion of introducing a comprehensive and most importantly uniform set of rules instead of the many national solutions[167] which have developed over the years, has been received favourably as it would ensure more legal certainly for platform providers.[168] In this thesis, the question arises whether this new framework will also apply to providers of Personal Information Management Systems.

I. Scope

As per Art. 2(1) DSA, the Regulation applies to intermediary services offered to recipients located in the European Union. The term

---

[166] *Busch/Mak*, 3 EuCML 2021, 109, 109; Heldt, in: Digital Platform Regulation, 69, 71; Carvalho/Arga e Lima/Farinha, 3 RDTec 2021, 71, 74.

[167] *Heldt*, in: Digital Platform Regulation, 69, 70f.

[168] *Janal*, 2 ZEuP 2021, 227, 231; *Busch/Mak*, 3 EuCML 2021, 109, 109; *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 75.

is, however, not to be confused with intermediation services as defined in Art. 2 No. 11 of the Data Governance Act. The definition of intermediary services was laid down in Art. 3(g) DSA. Its applicability to Personal Information Management Systems thereby needs to be assessed separately.

1. Information Society Services

First, the service needs to be considered an information society service in the meaning of Article 1(1), Point (b), of Directive (EU) 2015/1535, which defines such as *"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"*. In the context of Personal Information Management Systems, the characteristics of *"at a distance", "by electronic means",* and *"at the individual's request of a recipient*" can easily be affirmed. Potentially open would only be whether the service is in fact provided *"for remuneration"* if the use of the platform was, for example, offered for free. Here the DSA follows the approach of the E-Commerce Directive of excluding non-commercial service offerings from the regime.[169] As has, however, already been established in the context of analysing the ePrivacy Directive previously (see Part 2 Chapter 6: A. I. 1. For Remuneration, the CJEU has supported a broad understanding of the term. [170] Based on the existing case law, economic activities financed through other parties or means are also generally to be considered as provided "for remuneration".[171] Typical examples will include instances

---

[169]*Spindler*, 4 GRUR 2021, 545, 547; *Janal*, 2 ZEuP 2021, 227, 234; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 4; *Raue/Heesen*, 49 NJW 2022, 3537, 3537.

[170]C-339/15 *Vanderborght* [2016] ECLI:EU:C:2016:660, para 36; C-291/13 *Papasavvas* [2014] ECLI:EU:C:2014:2209, para 26; Case C-484/14 *Mc Fadden* [2016] ECLI:EU:C:2016:689, para 41; Case 352/85 *Bond van Adverteerders* [1988] ECLI:EU:C:1988:196, para 16.

[171]C-339/15 *Vanderborght* [2016] ECLI:EU:C:2016:660, para 36; C-291/13 *Papasavvas* [2014] ECLI:EU:C:2014:2209, para 26; Case C-484/14 *Mc Fadden* [2016] ECLI:EU:C:2016:689, para 41; Case 352/85 *Bond van Adverteerders* [1988] ECLI:EU:C:1988:196, para 16.

where a service is technically provided free for the recipients but revenue is generated through advertisements.[172] Based on this reading, Personal Information Management Systems offered to data subjects for free will still predominantly fall under that definition since they will typically either charge the controllers or establish an alternative business model, allowing them to profit economically to some extent.[173] It should, however, be noted that pure pro-bono or research projects such as the Advanced Data Protection Control[174] or Plus Privacy[175] might be excluded from the scope.

2. Intermediary Services

Art. 3(g) further provides for three types of information society services that are considered "intermediary services" under the DSA. It is important to note that this listing is not exemplary but rather enumerative and that services which do not fall under one of the listed categories will also not be within the scope of the Regulation.[176]

a) Categories

The types of intermediary services listed in Art. 2(g) are (1) mere conduit services; (2) caching services; and (3) hosting services.

Mere conduit services are described as *"consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*" (Art. 3(g)(i) DSA). Some examples are listed within Recital 29 of the DSA such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-

---

[172]C-291/13 *Papasavvas* [2014] ECLI:EU:C:2014:2209, para 30; Case C-484/14 *Mc Fadden* [2016] ECLI:EU:C:2016:689, para 43; Case 352/85 *Bond van Adverteerders* [1988] ECLI:EU:C:1988:196, para 16.

[173]*Spindler*, 4 GRUR 2021, 545, 547; *Janal*, 2 ZEuP 2021, 227, 234.

[174]Advanced Data Protection Control, https://www.dataprotectioncontrol.org/ (accessed: 23 October 2025).

[175]PlusPrivacy, https://plusprivacy.com/ (accessed: 23 October 2025).

[176]Hofmann/Raue / *Hofmann/Raue*, Art. 3 DSA, para 61; Kraul / *Nathanail*, § 2, para 17; *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 71-77.

level domain name registries, registrars, certificate authorities that issue digital certificates, voiceover IP, and other interpersonal communication services. What is important is that the provider may not modify the information in question or "be involved" with it in any form, in order to fall under the term (Recital 21 DSA). This, however, does not exclude the possibility of technical manipulations (Recital 21 DSA).

Under Art. 3(g)(ii) DSA, caching services also comprise the transmission of information provided by the recipient in a communication network. In contrast to mere conduit services they do, however, include automatic, intermediate, and temporary storage of such.[177] Furthermore, they need to be provided in order to assure that the information's onward transmission to other recipients is made more efficient.[178] Recital 29 DSA lists the sole provision of content delivery networks, reverse proxies or content adaptation proxies as generic examples of such.

Last but not least, hosting services consist of the storage of information provided by the service recipient and at their request (Art. 3(g)(iii) DSA). As per Recital 29 DSA, typical examples will include services such as cloud computing, web hosting, paid referencing, or services which enable the storage and sharing of information.

b) Applicability to PIMS

It is without a doubt that many of the described functionalities might also be present within a Personal Information Management System. For example, in order to ensure security when transmitting datasets from the data subject to the controller, a VPN might be used. Also, the possibility of verifying the individual's identity, thereby in a sense "certifying" it, has been discussed (see Part 1 Chapter 2: D. II. 1. b) cc) Perspectives for Advancements). A PIMS provider may block certain types of requests based on the user's preferences or

---

[177]Kraul / *Nathanail*, § 2, para 23.
[178]Kraul / *Nathanail*, § 2, para 23.

redirect requests, for example, in cookie consent to their server. Furthermore, as has been extensively explored in Part 1 Chapter 2: A. Storage, they will frequently store the data subject's information both in public or private clouds and enable the further sharing of such. These types of inclusions of functionalities will, however, always be accompanied by other core functionalities which make up the actual service. A PIMS will never be a "pure" intermediary service since, per definition, its purpose goes beyond the isolated intermediation. Its aim is, after all, to support the individual in the exercise of their rights and not simply to act as an uninvolved intermediary. It is therefore questionable whether PIMS would fall within the scope of the Digital Services Act, even if certain elements of their functionalities might be covered within the categories outlined in Art. 2(g) DSA.

aa) Considerations based on the DSA

The problem of these types of "hybrid" service offerings is recognised within Recital 15 DSA which provides that where some services offered are covered by the Regulation and others not, or they are covered within different sections, the DSA should apply *"in respect of those services that fall within their scope"*. Some indication may also be found within Recital 29, which specifies that *"intermediary services may be provided in isolation, as a part of another type of intermediary service, or simultaneously with other intermediary services"*. On the one hand, this may be understood as implying that whenever an overall service includes functionalities falling under the definition of 2(g) DSA, the Regulation would need to apply to these elements. On the other hand, Recital 29 only seems to refer to combinations of various intermediary services, not the incorporation of such functionalities into a service offering with a different overarching purpose. Also, Recital 15, while talking about instances in which parts of a company's offerings falls under the DSA and other parts do not, is more likely to refer to instances where a corporation might have various independent offerings within their business model, rather than individual components of one overall service.

A differentiation between actual intermediary services which only include elements of these or are facilitated through such, is explicitly

recognised in Art. 2(2) DSA. There it is established that the Regulation does not apply to services which are intermediary services by themselves but simply provided through the use of such.[179] Practical examples are outlined within Recital 6 DSA and may include remote information technology services, transport, accommodation, or delivery services. While Art. 2(2) only explicitly mentions services or products by intermediary services but not considered such themselves, the Recital suggests a broadening of the extent of this exclusion since it also refers to *"situations where the intermediary service constitutes an integral part of another service which is not an intermediary service"* in the same context. In such instances, the Recital establishes that the requirements set out in Union or national law relating to such should not be affected as has been recognised by the case law of the Court of Justice of the European Union (CJEU).[180]

bb) Considerations based on CJEU Case Law

The reference to CJEU Case Law is likely to relate to the Judgements of *Uber Spain*[181] and *Airbnb Ireland*[182], in which the Court introduced a distinction between online platforms falling within the scope of the E-Commerce Directive and those which are outside of such.[183] In the case of Uber, the Court established that the company is to be considered "a service in the field of transport" under Art. 2(2)(d) of Directive 2006/123, rather than an "information society service" under Art. 1(2) of Directive 98/34.[184] Airbnb on the other

---

[179]Kraul / *Nathanail*, § 2, para 28.

[180]*Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 77; *Busch/Mak*, 3 EuCML 2021, 109, 110.

[181]Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain SL* [2017] ECLI:EU:C:2017:981.

[182]Case C-390/18 *Airbnb Ireland* [2019] ECLI:EU:C:2019:1112.

[183]*Busch/Mak*, 3 EuCML 2021, 109, 110; *Janal*, 2 ZEuP 2021, 227, 235; *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 77.

[184]Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain SL* [2017] ECLI:EU:C:2017:981, para 40.

hand was considered by the Court as an information society service[185] based on considerations such as the fact that they provide hosts with a format for advertising their deals,[186] that the platform is responsible for the collection of rent and the transfer of such to the host,[187] and that the platform is not indispensable for the provision of the connected accommodation services[188] Relevant in this context is, however, mainly the fact that in both cases the CJEU established that the intermediation service needs to form an *"integral part of the overall service"* in order to be classified as an information society service.[189] Consequently, it can be assumed that services in which the described intermediary element in the form of mere conduit, caching, or hosting services required under Art. 2(g) is only an ancillary element to the overall offering, would not fall within the scope of the Digital Services Act.[190] This element, however, cannot be easily concluded in Personal Information Management Systems. PIMS are defined as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*.[191] The general goal of data subject empowerment is inherently broad and does not say much about the specifics of the offering. The question therefore occurs whether the mere conduit, caching, or hosting services potentially included within the platform constitute an integral part of such or rather just an ancillary element.

---

[185]Case C-390/18 *Airbnb Ireland* [2019] ECLI:EU:C:2019:1112, para 64.

[186]ibid para 59.

[187]ibid para 61.

[188]ibid para 55.

[189]Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain SL* [2017] ECLI:EU:C:2017:981, para 40; Case C-390/18 *Airbnb Ireland* [2019] ECLI:EU:C:2019:1112, para 50.

[190]*Janal*, 2 ZEuP 2021, 227, 234; Kraul / *Nathanail*, § 2, para 25; *Spindler*, 4 GRUR 2021, 545, 547; Hofmann/Raue / *Hofmann/Raue*, Art. 3 DAS, para 17; *Busch/Mak*, 3 EuCML 2021, 109, 109.

[191]*EDPS*, Opinion 9/2016, para 4; *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

cc) Considerations for Specific PIMS

It first needs to be noted that a general statement cannot be made for all types of PIMS. Purely transparency enhancing tools such as, for example, the Polisis[192] or the Usable Privacy Project,[193] which only review privacy policies but are neither involved in the transmission or storage of the users' data, will clearly not be within the scope of the DSA. On the other hand, service offerings focused on the provision of secure cloud storage service, while arguably not considered a typical PIMS, certainly will. The most relevant from a practical perspective are, however, more holistic platforms which allow the individual to manage their dataflows as a whole including transparency, consent management, (likely) storage, and potentially even the option of managing data subject requests. Here, while the focus of the service may not entirely lie on the pure intermediation but rather on the creation of a privacy friendly and empowering environment for the user, the inclusion of the relevant intermediation functionalities will still likely be necessary for the provision of the overall service. Most consent management platforms are directly tasked with transferring personal data to the data controller. Also, even where the platform would just transmit the consent signal without the actual data, this would constitute the facilitation of a form of communication. The same will apply in the context of facilitating data subject requests, where the PIMS will not only be tasked with the communication of the individual's request to the controller but also with ensuring the continuing interaction between those parties, including potentially the transfer of personal data from the controller to the data subject, where rights such as the right to access, portability or to receive a copy are concerned. For these types of service offerings, it needs to be concluded that the Personal Information Management System could not function without the inclusion of mere conduit, caching, or hosting services, making these an integral part of the platform rather than just ancillary element.

---

[192] *Harkous and others*, USENIX 2018, 531, 531ff.

[193] *Sadeh and others*, Usable Privacy Policy Project, 3f.

II. Consequences

The rules and regulations put forward for intermediary services by the Digital Services Act are not only extensive but also quite heterogeneous since separate and varied obligations are outlined for different types of service offerings.[194] Additionally to the standard intermediary services defined subsequently, the categories of "online platforms" (Art. 2(i) DSA) and "online search engines" (Art. 2(j) DSA), as well as "very large online platforms and very large online search engines" (Art. 33 DSA) have been introduced.[195] Personal Information Management Systems will, however, not fall under any of those terms as they neither deal with search queries for websites, nor disseminate information to the public. Therefore, the requirements only applicable to these types of platforms will not be discussed, putting the focus onto the potential impact of the DSA in PIMS.

1. Obligations

Chapter III of the Digital Services Act introduces several due diligence obligations for all types of intermediation service providers.[196]

a) Oversight

Firstly, they need to designate points of contact for both the recipients of the service (Art. 12 DSA), and Member State authorities, the Commission, and the Board (Art. 11 DSA). Also, similarly to Art. 27 of the GDPR, service providers which do not have their main establishment in the EU but offer their services in one of the Member States need to designate a legal representative there (Art. 13(1)

---

[194] *Müller*, MMR 2022, 1007, 1009; *Spindler*, MMR 2023, 73, 74; *Dregelies*, 12 MMR 2022, 1033, 1035f; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 3.

[195] *Müller*, MMR 2022, 1007, 1009; *Dregelies*, 12 MMR 2022, 1033, 1035f; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 3.

[196] *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 79; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 3.

DSA). This essentially serves the purpose of making sure that affected individuals as well as authorities can contact the relevant provider, regardless of the location of the main establishment.[197]

b) Notices

Secondly, providers of hosting services are required to introduce mechanisms which allow the submission of notifications toward them, regarding the presence of illegal content on their service (Art. 16(1) DSA). These mechanisms need to be set up so that they support the submission of *"sufficiently precise and adequately substantiated"* notices (Art. 16(2) DSA). Once a notification has been submitted, the individual or entity should be notified of the receipt (Art. 16(4) DSA), as well as the final decision made for the content in question (Art. 16(5) DSA). The relevance of these notices should also not be underestimated as the liability of the hosting provider under Art. 6 will often depend on the presence of a prior notification and the actions taken upon its receipt.[198]

In Personal Information Management Systems, the question arises what such "illegal" personal data would constitute. Art. 3(h) of the DSA introduces a quite wide definition of "illegal content", including *"any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law"*. This means that both the illegality of the data itself and the illegality of processing of such would be covered.[199] For personal data managed through a PIMS, this might, on the one hand, refer to datasets which are in fact not the personal data of the user but for example, of third parties. If the user did not have a legal basis for the

---

[197] *Müller*, MMR 2022, 1007, 1008; *Dregelies*, 12 MMR 2022, 1033, 1036; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 7.

[198] *Dregelies*, 12 MMR 2022, 1033, 1036.

[199] *Gerdemann/Spindler*, 1 GRUR 2023, 3, 4; *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 78.

processing of such data this might, for example, amount to the content being considered “illegal”. Also imaginable are instances where the information is considered the personal data of the user but such personal data violates other laws. For example, content or work created by the user which amounts to plagiarism or violates the rights of third parties will still be considered that individual’s personal data (in the same vein as wrong answers during a test are), but would clearly be illegal and fall under Art. 16 of the DSA.

Based on that, the level of involvement of the PIMS provider will be substantially higher than expected. After all, current platforms clearly market themselves as neutral intermediaries with no control nor responsibilities concerning the data managed through them. Should they fall under the definition of data intermediaries under the Digital Services Act, they will, however, now be legally obliged to actively engage with the uploaded data should they receive a notification of illegality. This will either be in the form of a removal, where the claim in the notification is substantiated, or in the decision to retain it. Either way, the service provider will make a crucial decision regarding the continuation or cessation of the processing of personal data, effectively making them the controller in the meaning of Art. 4 No. 7 of the GDPR.

c) Transparency

Furthermore, the Regulation assigns a high level of importance to transparency related obligations.

aa) Statement of Reasons

Should the provider of a hosting service impose any restrictions because certain content is established as illegal or incompatible with the terms of use, they are required to provide a statement of reasons to the affected recipient (Art. 17(1) DSA). This is in order to transparently inform all involved parties not only of the final decision itself but also the reasoning behind it and the facts which have been taken into

account.[200] Under Art. 17(3) DSA, this statement of reason needs to include information concerning (a) the nature of the restriction; (b) the facts and circumstances on which the decisions was based; (c) the use of automated means in reaching the decision, where applicable; (d) where the content is considered illegal, the legal grounds, as well as the reasoning for this assumption; (e) where the content is considered incompatible with the terms and conditions, a reference to the contractual grounds; and (f) information on the possibilities of redress.

This requirement to justify one's decision again underlines that the final determination is left solely to the discretion of the service provider. This supports the previously explored conclusion that they would be the party solely determining the future of the processing activity in question and thereby both means and purposes. It should also be noted that Personal Information Management Systems will need to ensure that in the case of automated decision-making, both the requirements of Art. 15(2)(c) DSA, and Art. 22 of the GDPR are met.[201] This is especially relevant since data subjects may issue complaints both based on Art. 17 DSA and Art. 77 of the GDPR.

bb) Terms and Conditions

All providers' terms and conditions should transparently set out any restrictions imposed on the use of the service including policies, procedures, measures and tools used for content moderation, as well as internal complaint handling systems (Art. 14(1) DSA). Such restrictions, however, need to be carefully considered and applied in a diligent, objective and proportionate manner, taking into account the rights and interests of all involved parties (Art. 14(4) DSA). In the context of how information is to be provided, the DSA goes even further than the GDPR. Art. 14(1) therein sets out that this information needs to be provided not only in clear, plain, intelligible, and unambiguous language but also in a "user-friendly" and "publicly available in an easily accessible and machine-readable" form.

---

[200] *Müller*, MMR 2022, 1007, 1009.
[201] *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 83.

Here again, the transparency requirements and the reference to the proportionality of certain measures show much resemblance to the principles of processing personal data laid down in Article 5 of the GDPR.[202] While these principles theoretically apply to all parties involved in the processing of personal data, it is the controller who holds the responsibility of demonstrating the compliance with such (Art 5(2) GDPR). It would therefore make sense to assume that the controller would also be responsible for the transparent communication of any restrictions posed on the service under Art. 14(1) DSA. Furthermore, the hosting provider is not only tasked with the transparent communication of those measures but will also presumably make all critical decisions concerning such activities. As many of those will require the processing of users' personal data, this will amount to the determination of the means of processing personal data. The determination of purposes, on the other hand, can be directly derived from the fact that they relate to a legal obligation of the hosting provider. In turn, the hosting service will likely have to take the role of a controller for all activities laid down in the terms and conditions.

cc) Reports

Providers of intermediary services are also required to once a year publish reports on the content moderation which they have implemented during that period (Art. 15(1) DSA). These reports should include information such as (1) the amount of received orders categorised according to the concerned type of illegal content (Art. 15(1)(a) DSA); (2) the median time required to inform the issuing authority (Art. 15(1)(a) DSA); (3) the number of notices submitted based on Art. 16, categorised according to the alleged type of illegal content (Art. 15(1)(b) DSA); (4) the amount of notices submitted by trusted flaggers, including the type of action taken as a result (Art. 15(1)(b) DSA); (5) the amount of notices which have been processed by automated means, as well as the median time required to take action (Art. 15(1)(b) DSA); (6) information on content moderation measures

---

[202] ibid.

taken by the provider on their own initiative (Art. 15(1)(c) DSA); (7) the number of received complaints (Art. 15(1)(d) DSA); and (8) the extent to which content moderation is conducted by automated means (Art. 15(1)(e) DSA).

This requirement, in a sense, mirrors the principle of accountability enshrined in Art. 5(2) of the GDPR since the purpose essentially lies in demonstrating that content moderation was deployed sufficiently. The European Data Protection Supervisor even explicitly welcomed this provision as it is considered to further increase the transparency of content moderation practices including the processing of personal data necessary for such.[203] The preparation of these reports will, after all, also require the performance of additional processing activities in the form of collection and aggregating personal data for the purpose of sharing the necessary numbers. Here again the service provider and, in this case, the Personal Information Management System will have to take the role of a controller since both purposes (in the form of a legal obligation) and means (deciding on how the report is to be generated) are determined by them.

2. Enforcement

The enforcement of the rules introduced by the Digital Services Acts is largely left to the authorities, both on a national and European level.[204] Similarly to the enforcement regime under the GDPR, Chapter IV introduces a vast amount of measures which may be taken by such.[205] The main authorities entrusted with monitoring the compliance of providers with the Regulation are so-called Digital Service Coordinators.[206]These are, for example, allowed to perform audits and on-premise inspections (Art. 51(1) DSA), to accept commitments and order cessation of certain activities (Art. 51(2)(a) and (b) DSA),

---

[203]*EDPS,* Opinion 1/2021, para 33.

[204]Kraul / *Bartels*, § 5, para 5; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 3; *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 80.

[205]*Buiten*, 12 JIPITEC 2021, 361, 377.

[206]*Gerdemann/Spindler*, 1 GRUR 2023, 3, 3; *Carvalho/Arga e Lima/Farinha*, 3 RDTec 2021, 71, 80.

as well as impose fines and penalty payments (Art. 51(2)(c) and (d) DSA). The amounts of such allowed by the DSA are also quite dissuasive, with fines for failure of to comply with the Regulation allowed up to 6% of the annual worldwide turnover of the provider of intermediary services (Art. 52(3) DSA) and periodic penalties up to 5% of the average daily worldwide turnover or income of the preceding financial year (Art. 52(4) DSA).

The competences of the Digital Service Coordinators will however not be applicable where the Commission has started proceedings for the same infringement (Art. 56(4) DSA). This rule is in line with the tiered approach of the DSA, which introduced specific responsibilities based on the criticality and risks of certain services.[207] In that sense, the monitoring of providers of very large online platforms and very large online search engines is largely left to the Commission in Articles 65–80 of the DSA.[208] Based on that, however, this exception is irrelevant for Personal Information Management Systems which are extremely unlikely to fall under one of these categories. Article 61 of the Regulation also introduces an independent advisory group for Digital Services Coordinators called the European Board for Digital Services, which is supposed to advise Coordinators and the Commission on the achievement of the objectives outlined in the Act.

3. Liability

Where a provider of an intermediary service fails to meet the requirements set out by the Digital Services Act, recipients are given the right to seek, under Union and national law, compensation for any damages or losses they have suffered due to such an infringement by Article 54. While not explicitly mentioned, this should include both actual damages, as well as lost profit.[209] Where possible, in rem restitution could also be considered.[210] It is, however, important to

---

[207] *Gerdemann/Spindler*, 1 GRUR 2023, 3, 3.

[208] ibid.

[209] Hofmann/Raue / *Hofmann/Raue*, Art. 54 DSA, para 3 and 44.

[210] Kraul / *Bartels*, § 5, para 121; Hofmann/Raue / *Hofmann/Raue*, Art. 54 DSA, para 52.

note that since this right is only available to the platform user, third parties will not be able to make such a claim.[211] This means that only the data subject, who is the direct user of the PIMS platform, will be given the option to ask for compensation under the DSA. The possibilities for data controllers or other types of recipients are, on the other hand, dependent on whether they will also sign up to the platform. While many PIMS, especially in consent management, operate in a form where both data subjects and controllers sign-up to the respective platform,[212] this is not always the case.[213] This implication might in a sense be indirectly furthering the development of more privacy friendly platforms. As has been stated in Part 1 of this thesis (see Part 1 Chapter 2: C. IV. Interim Conclusions: Consent), the dependency on the cooperation of the controller in a sense hinders the sole focus on the interests of the data subject, since platform providers also need to consider business needs in order to create a commercially viable product. If, however, the exclusion of data recipients as actual users allowed them to exclude liability under the DSA, businesses might be more motivated to create more independent solutions.

What should also be mentioned in this context is the fact that the Digital Services Act largely follows the regime of the E-Commerce Directive in the sense of substantially excluding the liability for third-party content.[214] Liability for mere conduit services is excluded by Article 4(1) DSA where the provider does not initiate the transmission, nor select the receiver or select or modify the contained information. This will be highly relevant in consent management platforms if, for example, the data subject consented to a data transfer without having the actual right to do so. Similarly, Article 5(1) excludes the liability of caching services where the information is not modified by

---

[211] Hofmann/Raue / *Hofmann/Raue*, Art. 54 DSA, para 20.

[212] For example: MyDex, https://mydex.org/platform-services/ (accessed: 23 October 2025) and Meeco, https://www.meeco.me/ (accessed: 23 October 2025).

[213] For example: PRIVACY-AVARE (*Alpers and others*, in: CLOSER 2018, 589, 591f.)

[214] *Buiten*, 12 JIPITEC 2021, 361, 369; *Spindler*, MMR 2023, 73, 75; *Dregelies*, 12 MMR 2022, 1033, 1034; *Gerdemann/Spindler*, 1 GRUR 2023, 3, 5.

the provider; the conditions on access, as well as the rules regarding the updating of such, where complied with; there was no interference with the lawful use of technology; and the provider expeditiously removed or disabled the access of such upon obtaining knowledge on the necessity to do so. Finally, in hosting services, the liability for illegal activities or content is excluded where the provider does not have knowledge of such or expeditiously removed it or disabled access when gaining awareness (Art. 6(1) DSA). In that context it is, however, important to remember that a service provider hosting illegal content might be considered having actual knowledge or awareness in this context if they have received a notice under Art. 16.[215] In accordance with Art. 16(3), this will especially apply if the information provided to them in the notice allowed them to identify the illegality of an activity or information without the necessity for *"detailed legal examination".*

4. Effects of the Roles taken by the GDPR

The Digital Services Act does not mention the GDPR other than clarifying that it is without prejudice to the rules laid down by data protection law (Art. 1(10)(i) DSA). As has been established previously in this thesis, the various due diligence obligations, in particular the transparency measures introduced by the DSA, bear much resemblance to the principles laid down within Art. 5 of the GDPR. More importantly, they might affect the roles taken by intermediary service providers under the GDPR.[216]

Should providers of Personal Information Management Systems fall within the scope of the Digital Service Act, they will naturally have to meet its obligations. Some of the due diligence requirements, such as the creation of notification mechanisms, will entail the processing of the personal data of the individual putting forward the notification, as well as the user it concerns. After all, Art. 16(6) explicitly mentions the obligation of providers to *"process any notices that they receive"*. Furthermore, the hosting service needs to conduct an assessment

---

[215] *Gerdemann/Spindler*, 1 GRUR 2023, 3, 5.
[216] *Spindler*, MMR 2023, 73, 74.

and reach a decision on whether the content in question can remain on the platform or should be removed. This clearly makes up a determination of the means of processing. The determination of the purpose is, on the other hand, derived from the fact that these actions are conducted based on a direct legal obligation of the service provider. The same can be concluded for all other due diligence obligations required of intermediation services such as the decisions concerning restrictions imposed on the use of the service (Art. 14(1) DSA) or the generation of reports on content moderation (Art. 15(1) DSA). Should any of these responsibilities be outsourced to third parties, they will have to take the role of a processor under Art. 28 of the GDPR.

a) Effect on other Service Elements

While the establishment of controllership regarding these responsibilities can be easily concluded, there are still two very relevant issues which need to be resolved. First, the above established controllership technically only relates to the obligations under the DSA, not to any other services performed by the PIMS. This is explicitly supported by Recital 15, which states that if *"some of the services provided by a provider are covered by this Regulation whilst others are not, or where the services provided by a provider are covered by different sections of this Regulation, the relevant provisions of this Regulation should apply only in respect of those services that fall within their scope"*. Service elements of a Personal Information Management System which do not constitute an intermediary service offering will therefore not be subject to those requirements, leaving open the question of their legal designation.

As has been laid down in Part 2 Chapter 3: C. III. 3. d) ff) Fragmentation, one of the main outcomes of the CJEU Case-Law, in particular the ruling of *Fashion ID*, was the introduction of the so called "stage based" approach in designating the roles taken toward the

data subject.[217] As a result, controllership can be established for a specific part of a processing activity, while separating it from prior or subsequent actions.[218] In PIMS falling within the scope under the Digital Services Act, such a splitting would likely be transferred onto the different elements of the service offering. As a result, the argument could be made that while the obligations performed by a PIMS as an intermediary service would make them data controllers under Art. 4 No. 7 GDPR, this controllership would only extend to the processing activities related to those obligations outlined under the DSA. For all other service elements, the determination of the roles taken vis-a-vis the data subject would then again need to be made on a case-by-case basis. This is supported by the findings made in Part 2 (see Part 2 Chapter 4: E. Findings for Part 2), which also evidences that the consistent application of the rules established by CJEU Case Law would potentially lead to a splitting in roles taken by the Personal Information Management System, depending on specific functionalities.

b) Effect on Business Users

Another question which occurs in the context of the division of roles under the GDPR for Personal Information Management Systems, is the relationship between the PIMS provider and the business user. As has been concluded in Part 2 (see Part 2 Chapter 4: E. Findings for Part 2), Personal Information Management Systems might share responsibilities as joint controllers under Art. 26 GDPR with the entity interested in, or already processing, the data subject's personal information. This will apply to business models under which the data controllers also sign up onto the PIMS platform. This assumption of joint controllership will, however, essentially be excluded where the PIMS service offering makes up an intermediary service.

---

[217] *Becker and others*, 12 IDPL 2022, 207, 212; *Zalnieriute/Churches*, 83 MLR 2020, 861, 871-875; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Paun*, 9 EuCML 2020, 35, 37.

[218] Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

Article 2(2) of the DSA stated that the Regulation and its requirements do not apply to non-intermediary services, even if they are provided through the use of such. Since the "business user" or "end controller" will probably not be considered an intermediary service themselves, the due diligence obligations under the DSA naturally will not affect them. By clearly removing this responsibility from the business user, the DSA also directly excludes the possibility of those assuming joint controllership for any of these processing activities. The Personal Information Management System constituting an intermediary service will have to assume sole controllership for all processing activities resulting from requirements put forward by the Digital Services Act.

III. Interim Conclusions: Digital Services Act

Whether a Personal Information Management System will fall under the definition of an intermediary service established in Article 3(g) of the Digital Services Act will largely depend on the specific of the service offering. Tools which are at no point tasked with the transmission or storage of the users' data but, for example, provide automated reviews of privacy policies will not fall within the scope of the Regulation. Also, providers which do not offer services for any remuneration, including a lack of advertisement or other forms of income generation, will also not be affected. Most "holistic" platforms directed towards facilitating, storage, consent management, data subject rights, and transparency will, however, also be subject to the rules of the DSA since the included mere conduit, caching, or hosting services are likely to form an integral part of the platform rather than just an ancillary element.

While Personal Information Management Systems will not be subject to the strict obligations applicable to "online platforms" (Art. 2(i) DSA) and "online search engines" (Art. 2(j) DSA), or "very large online platforms and very large online search engines" (Art. 33 DSA), Chapter III of the DSA introduces several relevant due diligence obligations applicable to all intermediation service providers. First, a point of contact for service recipients, Member States authorities, the

Commission, and the Board needs to be designated. Second, mechanisms allowing the submission of notices concerning illegal content on the platform need to be introduced. In PIMS, these notices are likely to relate either to the eligibility of the conducted processing or the content of the data itself. The consequences of these notices are relevant on two levels. First, the liability under Art. 6 DSA might depend upon the hosting provider conduct. Second, the fact that the hosting provider is required to make a decision concerning the notified content essentially forces them into deciding on the means and purposes of the further processing of the relevant dataset, inevitably making them a data controller under Art. 4 No. 7 of the GDPR.

The DSA also introduces a number of transparency requirements. First, where restrictions are imposed based on the assumption of illegality of certain content, the provider should provide a statement of reasons to the affected recipient. Second, hosting services need to transparently set out any restrictions imposed on the use of the service, including policies, procedures, measures, and tools used for content moderation, as well as internal complaint handling systems within their terms of use. Finally, they are required to annually publish reports on the content moderation which they have implemented during that period. These transparency related obligations bear much resemblance to the transparency obligations found within the GDPR. They also underline the level of responsibility that providers are assigned in that regard. Most importantly, however, all processing activities related to the fulfilment of the intermediation service providers' obligations under the DSA should be considered as being performed in the function as a data controller under Art. 4 No.7.

This assumption of controllership will, however, only apply to the specific requirements put forward by the DSA. For other service elements, a determination on a case-by-case basis, in accordance with the CJEU case law, will still be necessary. In effect, the fragmentation of roles taken by PIMS towards the data subject is further supported. The same will also extend to the relationship between the PIMS provider and other data controllers receiving data or coordinating the communication with the data subject through the platform. Since Art. 2(2) excludes any responsibility for non-intermediary services, even when they are provided through such, the parties will not

be able to agree on a joint controllership. The PIMS provider will therefore need to remain the sole data controller for all processing activities resulting from the performance of obligations introduced by the Digital Services Act.

Regarding the liability of such service providers, the DSA puts much focus on the actions of supervisory authorities on both national and European level. Those are namely the Digital Service Coordinators, the European Board for Digital Services, and the European Commission. The possibility of enforcement by individual users is limited to Article 54. It provides that recipients are given the right to seek under Union and national law compensation for any damages or losses they have suffered because of infringements of the Act. In contrast to Art. 82 of the GDPR, this right is only available to platform users and not third parties.

F. Digital Markets Act

Regulation (EU) 2022/1925 of the European Parliament and of the Council of September 14, 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, also referred to as the Digital Markets Act (DMA), came into force on November 1, 2022 and became applicable on May 2, 2023.[219] Together with the previously analysed Data Governance Act, Data Act, and Digital Services Act, it forms part of the European Union's Digital Agenda for 2020–2030.[220] It is intended to support the proper functioning of the internal market by establishing rules for the digital sector and ensuring its contestability and fairness (Recital 7 DMA).

---

[219] *Kraul/Schmidt*, 6 CCZ 2023, 177, 183; *Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3249; *Brauneck*, 1 RDi 2023, 27, 27.

[220] *Kraul/Schmidt*, 6 CCZ 2023, 177, 177; *Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3249.

I. Scope

At the heart of the Regulation lies the term of the "gatekeeper".[221] As per Article 2 No. 1 DMA, the term gatekeeper means *"an undertaking providing core platform services, designated pursuant to Article 3"*. Art. 3(1) of the DMA further specifies that these undertakings should (a) have a significant impact on the internal market; (b) provide core platform services, constituting an important gateway for business users to reach end users; and (c) enjoy an entrenched and durable position in its operations which is not likely to change in the foreseeable future. The focus on these is based on the observation that the current platform-economy is characterised by a significant degree of user dependence on a limited amount of providers, as well as inherent unfairness and imbalance between the parties.[222] The Regulation is intended to change these power structures and in a sense "level the playing field" for small and medium-sized businesses as well as end users.[223] The potential applicability of the Digital Markets Act to Personal Information Management Systems should therefore be considered.

1. Core Platform Services

The types of core platform services which fall within the scope of the Digital Markets Act are exhaustively listed in Article 2 No. 2.[224] These are namely: online intermediation services; online search engines; online social networking services; video-sharing platform services; number-independent interpersonal communications services; operating systems; web browsers, virtual assistants; cloud compu-

---

[221] *Kraul/Schmidt*, 6 CCZ 2023, 177, 183; *Colomo*, 12 JECLAP 2021, 561, 562.

[222] *Crémer and others,* 40 YALE J. ON REGUL. 2023, 973, 975; *Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3249; *Colomo*, 12 JECLAP 2021, 561, 563; *Brauneck*, 1 RDi 2023, 27, 27f.

[223] *Crémer and others,* 40 YALE J. ON REGUL. 2023, 973, 975; *Colomo*, 12 JECLAP 2021, 561, 563; *Brauneck*, 1 RDi 2023, 27, 28.

[224] *Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3250; *Colomo*, 12 JECLAP 2021, 561, 563.

ting services; and online advertising services, including any advertising networks, advertising exchanges, and any other advertising intermediation services provided by an undertaking that provides any of the core platform services.

While PIMS will not typically fall within that category, certain service elements might in fact be considered as a type of virtual assistant or communication service. Pure storage solutions might also be cloud computing services and transparency enhancing technologies that solely translate privacy policies or advise on the selection of data controllers without actually facilitating the sharing of data, could be considered as a type of virtual assistant. Also, where for example a consent management platform is also intended to facilitate a transactions (this could be imaginable if the idea of monetising ones personal data is further pursued), the platform might be considered a intermediation services.

2. Designation

Additionally, to being a core platform service, the Personal Information Management System would also need to be designated as a gatekeeper in accordance with the procedure laid down in Article 3 (Art. 2 No. 1 DMA). Such a designation is conducted by the Commission, based on both quantitative (Art. 3(4) DMA) and qualitative criteria (Art. 3(8)DMA).[225] On September 6, 2023 six gatekeepers were initially designated, namely: Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft.[226] The list was further expanded both on April 29, 2024, through the inclusion of iPadOS and on May 13, 2024 with the addition of Booking as a gatekeeper for its online intermediation service Booking.com. [227] Overall, 24 core platform services provided by these companies have been selected.[228] Functionalities enabling

---

[225]Podszun, *Käseberg/Gappa*, Art. 3, para 3.

[226]*European Commission*, 'Gatekeepers' <https://digital-markets-act.ec.europa.eu/gatekeepers_en> accessed 23 October 2024.

[227]ibid.

[228]Google Play, Google Maps, Google Shopping, Google Search, YouTube, Android Mobile, Alphabet's online advertising service, Google Chrome, Amazon

data portability which might bear some resemblance to Personal Information Management Systems, such as Google Takeout, Facebook's Transfer Your Information or Apple's Data Privacy page, have not been included. Neither has the joint venture of Apple, Meta, and Google, the Data Transfer Initiative.[229]

A designation by the Commission would be possible under Art. 3(1) if the undertaking in question had a significant impact on the internal market, provided an important gateway for businesses to reach end users, and enjoyed an entrenched and durable position in its current or foreseeable operations. Businesses meeting the financial thresholds under Art. 3(2) are presumed to hold such a position.[230] Since at the moment no providers of Personal Information Management Systems meet the turnover or user numbers established therein, the qualitative criteria of Art. 3(1) need to be applied.[231] These are mainly directed towards determining whether the service provider possesses a significant level of market power which would require the introduction of corrective measures in order to ensure fair and balanced competition.[232]

Pure storage solutions will automatically be excluded from the scope since these do not supply any sort of gateway for businesses to reach end users. The same will apply to services directed at the facilitation of data subject rights, since those are only relevant where a relationship between the individual user and the company (data controller) already exists. These are, therefore, directed at managing

---

Marketplace, Amazon Advertising, Apple AppStore, iOS, iPadOS, Safari, Tik Tok, Facebook Marketplace, Facebook, Instagram, WhatsApp, Facebook Messenger, Meta Ads, LinkedIn, Windows PC OS, Booking.com. See: DMA Website, https://digital-markets-act.ec.europa.eu/gatekeepers_en (accessed: 23 October 2025).

[229]Data Transfer Initiative, https://dtinit.org/(accessed: 23 October 2025).

[230]*Kraul/Schmidt*, 6 CCZ 2023, 177, 184; *Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3250.

[231]*Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3250.

[232]*Colomo*, 12 JECLAP 2021, 561, 561; *Schweitzer/Metzger*, 4 GRUR Int. 2023, 337, 343; *Podszun/Bongartz/Kirk*, 45 NJW 2022, 3249, 3250.

an existing connection, rather than allowing the formation of one. Potentially meeting the stipulation of Art. 3(1)(b) are, however, consent management functionalities as well as transparency enhancing tools which include a recommendation regarding the selection of the most privacy friendly controller. Here, the PIMS would in fact facilitate the creation of a relevant gateway for business users to reach end users. The question arises as to what extent this gateway is in fact "important". Here Recital 20 provides some details by specifying that a "*very high number of business users that depend on a core platform service to reach a very high number of monthly active end users enables the undertaking providing that service to influence the operations of a substantial part of business users to its advantage and indicate, in principle, that that undertaking is an important gateway*". In that context, it should be noted that at the moment, none of the reviewed Personal Information Management Systems on the market would be considered as having a high amount of business users dependent on reaching a high number of active end users. Most service offerings are in fact still in the development phase and even those that are fully functioning and usable do not have any significant influence.

The additional requirement of having a significant impact on the market (Art. 3(1)(a) DMA) and enjoying an entrenched and durable position in its operations (Art. 3(1)(b) DMA) will also not apply to the currently available PIMS. None of the reviewed tools can be considered as having a particularly strong market position, in contrast to the other providers. As of now, there is also no indication that this state of matters is about to change within the foreseeable future. In fact, the situation is quite the opposite; with the recently observed rise in AI Tools, the interest in PIMS seems to have significantly diminished over the past years. While this may change over time, the stipulations of the Digital Markets are, as of the time of writing, of no relevance for Personal Information Management Systems and will therefore not be further reviewed in this context.

II. Interim Conclusions: Digital Markets Act

While Personal Information Management Systems might fall within the terminology of core platform services, they do not hold sufficient market power to be considered as gatekeepers under the Digital Markets Act. The stipulations therein are therefore currently not relevant for PIMS providers. Based on current market trends, this is also unlikely to change in the foreseeable future.

G. AI-Act

In addition to the previously mentioned "Data Strategy", the European Union has also developed an "AI Strategy".[233] In April 2021, the European Commission published its Communication Fostering a European Approach to Artificial Intelligence,[234] its Regulatory Framework Proposal on Artificial Intelligence,[235] as well as an Impact Assessment of the Regulation on Artificial Intelligence.[236] It also reviewed its Coordinated Plan on Artificial Intelligence.[237] The intention behind this was to support the development of AI in Europe while

---

[233] *European Commission*, 'A European approach to artificial intelligence' https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed 23 October 2024).

[234] *European Commission*, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Fostering a European approach to Artificial Intelligence', https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2021%3A205%3AFIN (accessed 23 October 2024).

[235] *European Commission*, 'AI Act' <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (accessed 23 October 2024).

[236] *European Commission*, 'Impact Assessment of the Regulation on Artificial intelligence', https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence (accessed 23 October 2024).

[237] *European Commission*, 'Coordinated Plan on Artificial Intelligence 2021 Review', https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review (accessed 23 October 2024).

ensuring that these new technologies do not pose a risk for the rights and freedoms of individuals and society as a whole.[238]

On July 12, 2024 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, also referred to as the Artificial Intelligence Act or AI Act, was published.[239] The new rules are intended to ensure that Artificial Intelligence used and developed in the EU respects the rights and values fostered by the community in particular concerning safety, privacy, non-discrimination and transparency, as well as social and environmental well-being.[240] While Personal Information Management Systems are not primarily AI-driven, some tools, especially from the field of transparency enhancing technologies, already use techniques such as natural language processing as part of their service offering.[241] Since the current rise of the importance AI is not only undeniable but also likely unstoppable,[242] it should be assumed that such technologies will also gain more relevance in the context of PIMS. Based on this, the potential

---

[238] *European Commission,* 'A European approach to artificial intelligence', https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed 23 October 2024); *Hacker/Berz*, 8 ZRP 2023, 226, 226; *Mylly*, 54 IIC 2023, 1013, 1013; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 1; *Heiss*, 10 EuCML 2021, 252, 252.

[239] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] *OJ L, 2024/1689* (Artificial Intelligence Act).

[240] *Mylly*, 54 IIC 2023, 1013, 1013; *Hacker/Berz*, 8 ZRP 2023, 226, 226; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 1.

[241] *Hacker*, Datenprivatrecht, 567; *Pałka/Lippi*, in: Big Data Law, 115, 115ff; *Tesfay and others*, in: IWSPA '18, 15, 17; *Sadeh and others*, Usable Privacy Policy Project, 3f.

[242] *Hacker/Berz*, 8 ZRP 2023, 226, 226; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 1; *Hacker*, 13 Law, Innovation and Technology 2020, 257, 257.

applicability of the AI Act (AIA) and the related consequences should be considered.

I. Applicability

In accordance with Art. 2(1) AI Act, the Regulation applies to a number of actors including (a) providers placing on the market or putting into service AI systems; (b) deployers of AI located in the EU or having a place of establishment there; (c) providers and deployers from third countries, if the produced output of the AI is used in the EU; (d) importers and distributors; (e) product manufacturers placing or putting into service an AI system with their products; (f) authorised representatives of providers which are not established in the Union; and (g) affected persons that are located in the Union. The definition of an "AI system" can be found in Art. 3(1) AI Act. It refers to machine-based systems designed to operate with a certain level of autonomy which might exhibit adaptiveness after deployment. Further such systems need to infer how to generate output *"such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"* from the received input for either explicit or implicit objectives. It should be noted that this definition has changed significantly in comparison to the initial draft, which was likely based on the substantial criticism voiced by many sources who previously found the scope to be too broad.[243]

1. PIMS as AI-Systems

As has been established in Part 1 of this thesis, transparency enhancing technologies offering an "interpretative functionality" (see Part 1 Chapter 2: B. II. 1. Interpretative) often rely on a combination

---

[243] *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 2; *Hacker/Berz*, 8 ZRP 2023, 226, 227; *Heiss*, 10 EuCML 2021, 252, 252.

of natural language processing and either supervised or unsupervised machine learning.[244] This is largely based on the fact that manually reviewing all policies would simply be impossible. In those types of systems, the user might for example provide the URL where a specific privacy policy can be found or simply copy-paste its content into the tool.[245] The Personal Information Management System will subsequently create an overview of the processing activity in a transparent and user-friendly manner by means such as re-organising and categorising it, [246] only presenting information relevant to the specific individual, [247] or using visual means, such as specific colouring or icons.[248] This certainly amounts to the generation of output and can also be seen as a form of influencing the users' decisions (or at least attempting to do so), especially for tools which provide the data subject with a rating of the privacy practices described within the policy or direct recommendations for the use of privacy friendly controllers.[249] Similar technologies have also been used for the development of so called "auditing" transparency enhancing technologies, which review privacy policies based on their accuracy[250] or compliance with the applicable legal requirements.[251]

While the other types of Personal Information Management Systems reviewed for this thesis did not in effect generate their outputs

---

[244] *Hacker*, Datenprivatrecht, 567; *Pałka/Lippi*, in: Big Data Law, 115, 115ff; *Tesfay and others*, in: IWSPA '18, 15, 17; *Sadeh and others*, Usable Privacy Policy Project, 3f.

[245] *Harkous and others*, USENIX 2018, 531, 533-535; *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3; *Liepina and others*, in: ASAIL 2019, 1.

[246] *Harkous and others*, USENIX 2018, 531, 533-535.

[247] *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3.

[248] *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 2; *Harkous and others*, USENIX 2018, 531, 537f; *Tesfay and others*, in: IWSPA '18, 15, 19.

[249] *Harkous and others*, USENIX 2018, 531, 537f; *Zaeem/German/Barber*, 18 ACM Trans. Internet Technol. 2018, 1, 3.

[250] *Zimmeck and others*, PoPETs 2019, 66, 67; *Austin and others*, Towards Dynamic Transparency, 15f.

[251] *Contissa and others*, CLAUDETTE meets GDPR, 15.

based on inferences from the received input, nor did they operate autonomously to any extent, the future use of AI technology within PIMS should not be excluded. There are, after all, several possibilities through which PIMS could be made more efficient if certain AI solutions were adequately applied. First, the possibility of a more automated handling of consent requests might be considered. It is, for example, imaginable that the data subject would set up their generalised privacy preferences which would then be applied and managed for all controllers by an accordingly trained tool. On the one hand, the validity of such consent might be legally challenged, considering that Art. 4 No. 11 GDPR technically requires an affirmative action directly from the data subject.[252] Based on that, some sources have spoken against the possibility of allowing any type of representation in the exercise of the right to privacy.[253] The prevailing opinion, however, does not follow that notion and ascertains that the possibility of deciding to be represented by a third party is included within the right to informational self-determination.[254] This can also be concluded based on Art. 80, which clearly intends to open the possibility for data subjects to be represented by third parties in the exercise of their rights.[255] Furthermore, the sheer allowance of consent management tools already supports the notion that the data subject may choose to have their will executed by a selected provider.[256] This kind of "outsourcing" might therefore, at least potentially, also be exercised through the use of an AI-based technology.

Should that be the case, the requirements of Art. 22 GDPR will also have to be taken into account. Automated decisions on user consent will arguably amount to producing a legal or similar effect.

---

[252] *Kühling/Sauerborn*, 10 ZD 2022, 531, 533; *Botta*, 12 MMR 2021, 946, 948; *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, 6 MMR-Beil 2021, 25, 41.

[253] *Ulmenstein*, 44 DuD 2020, 528, 532.

[254] *Kühling/Sauerborn*, 10 ZD 2022, 531, 533; *Botta*, 12 MMR 2021, 946, 948; *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, 6 MMR-Beil 2021, 25, 41; *Kühling*, 45 DuD 2021, 783, 784.

[255] *Botta*, 12 MMR 2021, 946, 948; *Kühling*, 45 DuD 2021, 783, 785.

[256] *Kühling*, 45 DuD 2021, 783, 784.

Still, this should not be considered as a significant hurdle since the exemptions of Art. 22(2)(a) and (c) could be applied. On the one hand, there might be instances where the entire service offering of the PIMS is AI-based, with no alternatives. Here, if the data subject wished to use this particular tool, the use of AI would clearly be necessary for the performance of the contract (such as a subscription to or purchase of the PIMS) between the parties. On the other hand, there might be instances where the service could be provided without the use of automated decision-making. For example, a PIMS might offer both the possibility of automated and manual consent management. This could similarly apply if the tool included multiple modules (such as consent management, storage or portability) which can be purchased separately. In both instances, the user would have a genuine free choice between the various possibilities, allowing the applicability of Art. 22(2)(c) where Art. 22(2)(a) cannot be selected.

Even more promising are, however, the possibilities of using artificial intelligence for managing data subject requests. As has already been established in Part 1 of the thesis, the currently available solutions in that regard are far from satisfactory (see Part 1 Chapter 2: D. II. 1. b) cc) Perspectives for Advancement). There are multiple potentials for advancements based on existing technologies. One considered solution was the adoption of natural language processing methods applied in transparency enhancing tools in order to audit the content and accuracy of the answers to access requests provided by the controller. Here, the use of an automated reply system, flagging any inaccuracies to the business in question, was further suggested. Within the last years we have also observed huge developments in generative AI by tools such as ChatGPT and GPT4.[257] Similar technologies could be used on order to generate the content of a request automatically, based on instructions provided by the data subject. Furthermore, presented issues in relation to locating the relevant datasets in order to comply with deletion or rectification re-

---

[257] *Helberger/Diakopoulos*, 12 IPR 2023, 1, 2; *Strowel*, 54 IIC 2023, 491, 491; *Hacker/Berz*, 8 ZRP 2023, 226, 226.

quests (see Part 1 Chapter 2: D. II. 3. c) Technical Execution, Challenges and Potential for Advancements) may also be supported by logic- and knowledge-based approaches. Ideally, such solutions would even be able to directly employ the necessary changes.

2. Role of the PIMS

The AI Act differentiates between several parties which can be included in the process of developing and deploying an AI system. The most relevant ones are providers (Art. 3 No. 3 AIA), deployers (Art. 3 No. 4 AIA), importers (Art. 3 No. 6 AIA), and distributors (Art. 3 No. 7). Addressing all of these stakeholders and regulating the extent of their accountability is necessary, since especially in the case of developing AI systems, there are often a multitude of entities involved. [258] The differentiation between these roles is also significant since the AI Act creates different responsibilities for each of the parties with regards to varying types of systems. Whereas some obligations are assigned to all of the actors with regards to High-Risk Systems,[259] only providers and deployers are subject to the transparency obligations outlined for certain AI systems under Art. 50 AIA. In the context of PIMS, the question naturally occurs what type of role might be applicable.

In accordance with Art. 3 No. 3 AIA, a provider is the entity which develops the AI system (or had it developed) and subsequently places it on the market or puts it into service under their own name. A deployer is the entity using the AI system under their authority (Art. 3 No. 4 AIA). Both of these roles could potentially be relevant for a Personal Information Management System. On the one hand, a PIMS provider could develop their own AI-based functionalities within the PIMS and put it on the market. On the other, they may use an existing system and integrate it into their application, thereby making them the deployer. In that sense, all types of obligations might

---

[258] *Hacker/Berz*, 8 ZRP 2023, 226, 228.

[259] For example, the obligations of providers are primarily outlined in Art. 16-23 AIA; for product manufacturers in Art. 24 AIA; for importers in Art. 26 AIA; for distributors in Art. 27 AIA and for users in Art. 29 AIA.

potentially apply. Still, the type of duties enshrined for providers and developers of AI systems predominantly depend on the type of system. The applicability of those rules to PIMS will therefore be discussed separately.

II. Consequences

It is clear that there are not only Personal Information Management Systems which would be considered AI systems under the AI Act. It is also more than likely that the numbers of these will increase in the future. This, however, is not to say that all stipulations of the Regulation will automatically apply to all PIMS. The AI Act follows a risk-based approach and essentially divides AI-Systems into four categories, based on which the respective obligations and the potential penalties are determined. [260]

1. Obligations

The four types of AI systems established by the AI Act are: strictly prohibited AI practices; high-risk AI systems, which are subject to a large amount of obligations; certain types AI systems, subject to transparency requirements; and those who do not fall under any of the other categories and thereby have no responsibilities under the AI Act.[261]

a) Prohibited Systems

The first are artificial intelligence practices which are entirely prohibited under Art. 5 AI Act.[262] These are for example systems which

---

[260] *Hacker/Berz*, 8 ZRP 2023, 226, 226; *Helberger/Diakopoulos*, 12 IPR 2023, 1, 3; *Schuett*, 15 EJRR 2024, 367, 371; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 3; *Novelli and others*, 39 AI & Soc 2024, 2493, 2493f.

[261] *Hacker/Berz*, 8 ZRP 2023, 226, 226; *Helberger/Diakopoulos*, 12 IPR 2023, 1, 3; *Schuett*, 15 EJRR 2024, 367, 371; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 3; *Novelli and others*, 39 AI & Soc 2024, 2493, 2493f.

[262] *Hacker/Berz*, 8 ZRP 2023, 226, 226; *Heiss*, 10 EuCML 2021, 252, 255.

subliminally manipulate individuals into causing physical or psychological harm; exploit vulnerabilities of certain groups; evaluate the trustworthiness of individuals on behalf of or directly by public authorities; and to a large extent, real time remote biometric identification systems. These characteristics are clearly intended to prevent the use of systems posing a serious threat to the rights and freedoms of individuals and do not apply to any type of Personal Information Management Systems.[263]

b) High-Risk Systems

The second and most relevant type, are “high-risk” AI systems.[264] In accordance with Art. 6(1) AI Act, these are all systems that include a product subject to specific European Union harmonisation legislation listed in Annex I of the Act, or a safety component of such. The listed legislation includes areas such as the harmonisation of the safety of toys, components for lifts, pressure equipment, cableway installations, or medical devices. The second category of high-risk AI systems is established in Annex III (Art. 6(2) AI Act).[265] These are specific types of tools applied in areas such as biometrics, education, critical infrastructures, employment, law enforcement, border control management, migration, or the administration of justice and democratic processes.[266]

Out of the listed categories, the only type which might relate to Personal Information Management Systems are those listed in Annex III No. 1, namely AI systems used for remote biometric identification of natural persons. As has been laid down under in Part 1 Chapter 2: D. I. 3. b) Identification of the Data Subject, ensuring the

---

[263]*Schuett*, 15 EJRR 2024, 367, 371; *Heiss*, 10 EuCML 2021, 252, 255.

[264]*Hacker/Berz*, 8 ZRP 2023, 226, 226; *Helberger/Diakopoulos*, 12 IPR 2023, 1, 3; *Heiss*, 10 EuCML 2021, 252, 255.

[265]Steinrötter / *Bastians*, '§ 21 Plattformspezifische Vorgaben des AI Act', para 40; *Schuett*, 15 EJRR 2024, 367, 371.

[266]Steinrötter / *Bastians*, '§ 21 Plattformspezifische Vorgaben des AI Act', para 40; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 3; *Heiss*, 10 EuCML 2021, 252, 255.

identity of the individual submitting a data subject request is crucial in managing such an enquiry. After all, any activities performed on a dataset (such as, for example, submitting details of the processing activities, erasing information or providing copies of personal data) based on a request of someone other than the data subject would constitute a breach in the meaning of Art. 4 Nr. 12 GDPR. Based on that, the possibility of using biometric identification procedures in order to truly confirm the individual's identity might be considered.

It should, however, be noted that the AI Act makes a clear differentiation between biometric identification and biometric verification (Recital 15 AIA). Point 1(a) of Annex III only refers to "remote biometric identification systems", which are defined under Art. 3 No. 41 AIA as *"an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database"*. This type of feature would, however, not appear within a PIMS verifying the identity of the individual for the purpose of managing a data subject request. After all, a data subject request will always need to be at least initiated by the individual, therefore excluding the possibility of being performed *"without their active involvement"*. The exclusion of PIMS functionalities used for the identification of an individual from the scope of High-Risk Systems is further underlined in the second sentence of Point 1(a) of Annex III. Here it is clearly stated that *"AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be"* would not be included within the scope. As a result, even if AI-based PIMS solutions would be used for the purpose of verifying the data subject's identity, they will not be high-risk AI systems in the meaning of Art. 6, AI Act and therefore also not be subject to the many stipulations and requirements[267] provided for such.

---

[267]For an overview of the applicable requirements refer to: *Schuett*, 15 EJRR 2024, 367, 375ff, 8-17; *Schwemer/Tomada/Pasini*, in: LegalAIIA 2021, 1, 6-8.

c) Certain AI-Systmes

Article 50 of the AI Act creates additional transparency obligations for certain types of AI systems. These are: (1) systems intended to interact with natural persons; (2) systems generating synthetic audio, image, video or text content; (3) emotional recognition or biometric categorisation systems; and (4) systems generating deep fakes. The creation of deep fakes or use of emotional recognition in Personal Information Management Systems seems highly unlikely. First, there does not seem to be any apparent advantage that would significantly improve the functionalities or user experience. Second, the PIMS provider would need to process a significant amount of personal data in order to use these types of techniques. This would, in a sense, go against the entire purpose of these "privacy friendly" tools. Data subjects might even be discouraged from selecting such a provider if they had the impression that they were dealing with an entity recklessly processing and analysing large amounts of personal data for no apparent purpose other than a more "entertaining" user experience. Furthermore, the legal regulation in the context of data intermediation generally requires these types of entities to act in a neutral manner and not use the user's personal data for own purposes. [268] Such a rule has, for example, been established in Art. 12 of the DGA, as well as § 26(2) No. 2 of the German TDDDG. While user's personal data may be used for the further development of the service (Art. 12(c) DGA), this exception should be applied in a restrictive manner. Based on the principle of purpose limitation, only processing strictly necessary for the further development of the service (Art. 5(1)(b) GDPR) should be allowed. Both emotional recognition and the creation of deep fakes, however, seem unlikely to fall under that category. While the types described under Art. 5(3) and (4) AIA will therefore not apply to PIMS, the applicability of Art. 5(1) and (2) does seem possible and should further be explored.

---

[268] *von Ditfurth/Lienemann,* 23 CRNI 2022, 270, 282.

aa) Systems Intended to Interact with Natural Persons

Certainly, applicable to providers of Perl Information Management Systems will, however, be Art. 50(1) of the AI Act. PIMS are per design intended to interact with the data subject. Should AI systems be used in any manner in that context, the individual will need to be transparently informed of that fact.

(1) Form

On the surface, this obligation does not seem to create much of a burden for providers. After all, any interaction with an automated tool by a natural person will logically involve the processing of that individual's personal data, regardless of whether AI is involved.[269] Therefore, the extensive transparency obligations of Art. 12 and 13 of the GDPR would apply either way. In that sense the requirement to add the clarification that AI is also being used would not really demand much additional effort. Art. 50(1) might however also be read as going beyond the right to information enshrined in the GDPR. The typical practice of providing details about processing based in Art. 12 and 13 of the GDPR involves the provision of privacy notices. Both research and practical experience have confirmed that these are certainly not effective and in fact, are rarely being read.[270]

Art. 50(1) explicitly asks for the system to be *"designed and developed"* in a manner that ensures the individual will be aware of the interaction with an AI component, arguably alluding to the principle of data protection by design and default, found in Art. 25 GDPR. Since the system's design should already integrate that information, the natural person will know about the use of AI from the sheer interaction and without having to consult any additional notices, information sheets, terms and conditions, or any other form of communication channel. The information would need to be available directly.

---

[269] *Ciancimino*, 5 EuCML 2022, 173, 175.

[270] *Choi/Park/Jung*, 81 Comput. Hum. Behav. 2018, 42, 42ff; *Tian/Chen/Zhang*, 12 Applied Sciences 2022, 9702, 4; https://jusletter.weblaw.ch/juslissues/2018/924/profiling-in-the-gdp_3b8e8a124f.html__ONCE&login=false (accessed: 04 March 2026); *Schaub and others*, SOUPS 2015, 3.

This clearly goes beyond the transparency obligations established in the GDPR, where consent notices regularly only contain a few minimal facts and refer to the second layer for more input.[271] This practice of leaving the data subject with the need to actively search out information is even more prevalent where legal bases for processing other than consent are being used.[272] In AI-based systems, the provider will therefore have the added burden of ensuring that the involvement of artificial intelligence is sufficiently clear right away. This is further supported by the fact that the only exemption refers to instances where the use of AI is *"obvious from the circumstance and the context of use"*.

(2) Content

While extending the requirements concerning the availability of information, Art. 50(1) AIA does not provide any details regarding the content of such, other than the fact that the user should be aware about the use of AI. There is no mention of having to explain the purposes of the AI, the types of data used for its functioning, or the manner in which decisions are being made. In that context, the transparency requirements under the GDPR might in fact be more stringent. As has already been established (see Part 3 Chapter 6: G. I. Applicability), the use of PIMS might in certain instances (such as automated consent management) amount to automated decision-making, producing legal or similar effects in accordance with Art. 22(1) GDPR. This means that the requirements for such a processing activity need to be considered. Based on both Art. 13(2)(f) and Art. 14(2)(g), data subjects have the right to receive information about the existence of automated decision-making, including *"meaningful information about the logic involved as well as the significance*

---

[271] *McDonald and others*, in: PET, 37, 53; *Gluck and others*, SOUPS '16, 321, 322; *Karegar/Pettersson/Fischer-Hübner*, 23 ACM Trans. Priv. Secur. 2020, 1, 2.

[272] CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC' para 97, https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf (accessed: 24 October 2025). Here the supervisory authority concluded that the provided information was excessively scattered and hard to access.

and the envisaged consequences of such processing for the data subject".

While not required by the AI Act, the PIMS provider will therefore be obliged to at least explain in general terms the rationale behind the functioning of the system, as well as any other details which might be deemed relevant by the individual user. [273] While this does not mean that a specific algorithm needs to be disclosed, the provided details need to be precise enough for the individual to understand the underlying logic, in order to exercise their rights under Art. 15–22 of the GDPR. [274] Whether these transparency provisions also provide data subject with a subjective right to an explanation is still heavily debated.[275] The Art. 29 WP seems to support that notion, with the underlining of the importance for the data subject to be able to *"understand the reasons of the decision"*.[276] Similarly, Recital 72 refers to the individual's right *"to obtain an explanation of the decision reached after such assessment and to challenge the decision"*. Furthermore, the notion of local explanations has been supported by some Member State courts.[277] Considering the comparative lack of protection for individuals where AI systems that are not considered "high-risk" are used, a broad interpretation of the right to information seems to be warranted in that regard.

(3) Provider

Also, quite relevant when comparing the transparency requirements of the AI Act with those enshrined in the GDPR is the question

---

[273] *Art. 29 WP*, Guidelines on Automated individual decision-making, 25; *Selbst/Powles*, 7 IDPL 2017, 233, 236; *Custers/Heijne*, 46 CLSR 2022, 105727, 5; Kuner and others / *Zanfir-Fortuna*, Art. 13, 414, 430.

[274] *Art. 29 WP*, Guidelines on Automated individual decision-making, 25; *Hacker/Passoth*, in: xxAI, 343, 349 *Selbst/Powles*, 7 IDPL 2017, 233, 236; *Custers/Heijne,* 46 CLSR 2022, 105727, 5.

[275] *Malgieri/Comandé*, 7 IDPL 2017, 243, 243 ff; *Wachter/Mittelstadt/Floridi*, 7 IDPL 2017, 76, 76ff; *Selbst/Powles*, 7 IDPL 2017, 233, 233ff.

[276] *Art. 29 WP*, Guidelines on Automated individual decision-making, 25.

[277] See for example: Rb. Amsterdam - C/13/689705/HA RK 20-258. Also: http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html (accessed: 13 March 2026).

of who should guarantee their realisation. The obligation to provide the data subject with all information relevant to the processing of their personal data under Art. 13 and 14 of the GDPR applies to the data controller, meaning the entity determining the means and purposes of processing personal data (Art. 4 No. 7 GDPR). The transparency obligations enshrined in the AI Act on the other hand apply to the "provider". This entity has been defined in Art. 3 No. 3 of the AIA as *"a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge"*.

The transparency obligations are therefore extended in two additional manners by including more parties obliged to its assurance and extending their relevance to the development phase. This has significant practical relevance. Since data processing is rarely a process involving simply one entity during all stages, the extension to parties other than the controller is quite welcome. After all, it is the developer of a tool who will actually have the means to implement privacy friendly solutions based on the principle of privacy by design and default (Art. 25 GDPR). Especially in the context of AI, there are often multiple entities involved in the process of development.[278] A controller, on the other hand, might be limited to selecting between various providers if they cannot create a new technology by themselves. The restriction of data protection obligations to controllers and to some extent processors prevalent in the GDPR essentially creates a gap in protection when it comes to the responsibilities of other relevant parties. The fact that the GDPR is silent on any liability on the side of developers and producers of products has in fact been a major point of criticism.[279] As a result, Personal Information Management Systems, where involved in the development of AI-based solutions,

---

[278] *Hacker/Berz*, 8 ZRP 2023, 226, 228.

[279] *Specht-Riemenschneider*, 2 MMR 2020, 73, 74; *Dahi/Corrales Compagnucci*, 47 CLSR 2022, 105762, 3f; *Banasiński/Rojszczak*, 7 J. Cybersecur. 2021, 1, 5; *Hacker*, Datenprivatrecht, 294.

will also be subject to the transparency obligations enshrined in Art. 50 AI Act, even if they were not to be considered controllers under Art. 4 No. 7 GDPR. The extension introduced in the AI Act is therefore both welcome and relevant for the future of Personal Information Management Systems.

bb) Systems Generating Audio, Image, Video or Text Content

Another category of "certain AI systems" introduced by Art. 50(2) AIA are those generating audio, image, video, or text content. As has been mentioned in the context of transparency enhancing technologies (see Part 1 Chapter 2: B. II. 1. Conflict of Objectives), the idea of using elements such as icons, [280] QR-codes, voice alerts, and videos for a more understandable presentation of privacy notices is explicitly supported.[281] Other elements such as visceral notices,[282] or comics[283] have also been considered. While these are not generated by an artificial intelligence as of the time of writing, it would at least be imaginable to have such elements included in the future. For example, based on a privacy notice, an AI system may be able to provide a short video explaining the processing to the data subject. Audio and visuals might also be automatically generated and used in the same manner. Further imaginable would be the creation of text content used for the submission of data subject requests, tailored towards the specific needs of the individual instead of using a preformulated text template. If an AI technology used by a PIMS fell under that category, the provider would need to ensure that the outputs were marked in a machine-readable format and that the fact that they were manipulated by AI was detectable (Art. 50(2) AIA).

---

[280] *Efroni and others*, 5 EDPL 2019, 352, 352ff; *Rossi/Palmirani*, in: Big Data Age, 181, 181ff; *Holtz/Zwingelberg/Hansen*, in: Privacy and Identity Management for Life, 279, 279ff; *Holtz/Nocun/Hansen*, 6th IFIP, 338, 338ff; *Geminn/Francis/Herder*, 14 ZD-Aktuell 2021, 05335.

[281] *Art. 29 WP*, Guidelines on transparency, para 39f.

[282] *Calo*, 87 Notre Dame Law Rev. 2013, 1027, 1034-1041.

[283] *Tabassum and others*, in: 2018 CHI Conference, 1ff; *Knijnenburg/Cherry*, SOUPS 2016.

The practical relevance of this category for PIMS is, however, likely quite limited. Art. 50(2) AIA also provides that these obligations do not apply where the system has simply performed an *"assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof"*. While a PIMS might therefore generate audio, images, videos, or texts for the data subject, the described possibilities are likely to fall within that exception. Any support in preparing data subject requests will likely amount to a purely assistive function. Similarly, any presentation of privacy notices in a visual or audio form would not really alter the input substantially but simply display it in a new manner. In that sense, the applicability of Art. 50(2) to PIMS is highly unlikely. Since in the described instances the system will be interacting with the data subject, the transparency obligations of Art. 50(1) will still apply.

d) General Purpose AI-Models

Furthermore, Chapter V of the AI Act establishes certain rules for so called "general-purpose AI models". Key elements of such models are their ability to perform a wide range of distinct tasks, display significant generality, and the fact that they can be integrated into a variety of systems or applications (Art. 3 No. 63). Personal Information Management Systems, on the other hand, serve a specific purpose and have specific, pre-defined functionalities before being put on the market. A PIMS provider can therefore, per definition, not be considered a provider of a general-purpose AI model.

2. Enforcement

Article 99 AIA establishes rules for imposing penalties for infringements of the Regulation. According to Article 99(3), the highest penalties may reach up to €35 million or 7% of a company's total worldwide annual turnover for the preceding financial year. Still, these amounts are unlikely to apply to Personal Information Management Systems as they are only awarded for non-compliance with the prohibition established for certain AI Systems in Art. 5. Potentially relevant for PIMS are, however, the still quite substantial amounts provided for in Art. 99(4) AIA. Based on this provision, the incompliance

with any other obligations laid down within the Act may be penalised with fines as high as €15 million Euro or up to 3% of a company's total worldwide annual turnover for the preceding financial year. PIMS failing to comply with the transparency obligations under Art. 50 could therefore potentially be fined with similar amounts, as they would under the GDPR be considered a controller.

The AI Act does not introduce any rules concerning civil liability. Claims will therefore need to be based on other laws and regulations, such as contractual liability and tort law.[284] This does not mean that specific risks arising from the use of AI systems and their effect on the traditional liability regime are ignored by the lawmakers. The establishment of liability rules for AI based systems is part of the European Commission's AI Strategy.[285] In its Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, the European Commission has identified specific challenges posed by AI-based systems to the current regime of liability.[286] In order to adequately address these, the European Commission had published a proposal for a new AI Liability Directive (AILD).[287] This proposal has however been withdrawn in October 2025.[288] While it is therefore not currently relevant, a quick look at its potential effects, might be interesting, in case it resurfaces at a later point.

---

[284] *Schuett*, 15 EJRR 2024, 367, 384; *Hacker*, 13 Law, Innovation and Technology 2020, 257, 268-271.

[285] *European Commission*, 'Liability Rules for Artificial Intelligence', https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en accessed 24 October 2024.

[286] *European Commission*, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' (19 February 2020).

[287] *European Commission*, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' COM(2022) 496 final.

[288] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive (accessed: 25 April 2026).

The AI Liability Directive largely followed the categorisation of different types of AI systems applied in the AI Act.[289] It also directly refered to the Act in the context of defining the crucial terms of "AI system"; "high-risk AI system"; "provider" and "user" (Art. 2 No. 1–4 AILD). These laws, together with the new Product Liability Directive mentioned above (see Part 1 Chapter 2: B. Product Liability Directive), were intended to complement each other.[290] Art. 1(1) AILD provided that the directive is intended to lay down rules for (1) the disclosure of evidence on high-risk AI systems; and (2) the burden of proof for claims for damages caused by AI in the context of non-contractual fault-based civil law claims. The first instances, which were regulated in Art. 3 AILD, are not relevant in the context of liability of Personal Information Management Systems since it has been established that those are extremely unlikely to be considered "high-risk" under the AIA. Furthermore, limited to high-risk systems are the rules of alleviation of the burden of proof established in Art. 4(2) and (4) AILD.

There are, however, some rules which applied to all types of AI systems and thereby also to PIMS, where such technologies are used. Art. 4(1) AILD laid down conditions under which the causality between the fault of a defendant and the output of an AI system or a failure of the system to produce the output is to be presumed. First, the defendant or a person for whom they are responsible needs to have violated a duty of care. Notably this includes any type of duty and is not restricted to obligations outlined within the AI Act.[291] Second, it needs to be "reasonably likely" that this violation would produce the output subject to the procedure. Third, the output in question has produced the damage. This reversal of the burden of proof between the fault and the output is largely based on the fact that it is often difficult, if not even impossible, to prove which specific element

---

[289] *Hacker*, CLSR 2013, 105871, 9.
[290] *Hacker*, CLSR 2013, 105871, 3; *Zech*, 22 ERA Forum 2021, 147, 150.
[291] *Hacker*, CLSR 2013, 105871, 33.

or feature of an AI system led to a specific result.[292] This is also why many scholars have in advance argued for the establishment of such rules for reversal.[293] It should, however, be noted that this presumption would have only applied where the court believes that it would be excessively difficult for a claimant to prove the causal link (Art. 4(5) AILD) or where a defendant, who used the system for personal activities, materially interfered with how the system operates or failed to determine the conditions of operation (Art. 4(6) AILD).

a) Duty of Care

Such issues will equally affect users of Personal Information Management Systems. As a result, should actions be performed by the platform which are against the preferences set up by the data subject, the individual would likely not have to prove the specific way in which the damages have been caused. Under Art. 4 (1)(a) AILD, this would only have applied where a specific duty of care is established in European Union or national law which is intended to protect against the type of damages that have occurred. Damages caused by PIMS are most likely to relate to the processing of the user's personal data, either in the form of lacking technical and organisational measures, erroneous data transfers, wrongful deletion, or essentially any type of data processing not intended by the data subject. The duty of care that needs to be established will therefore have to result from obligations enshrined in the GDPR. In practice, this might pose a problem. The GDPR essentially only creates responsibilities for the data controller and the processor and not for any other parties.[294] As has been explained in Part 2 of this thesis (see Part 2 Chapter 4:

---

[292] *Barredo Arrieta and others,* 58 IF 2020, 82, 83; *Panigutti and others*, FAccT '23, 1139, 1140.

[293] *Spindler*, in: Liability for AI and the IoT, 125, 138; *Sommer*, Haftung, 375-379; *Thöne*, Autonome Systeme, 257-261; *Zech*, Gutachten A, 60.

[294] *Specht-Riemenschneider*, 2 MMR 2020, 73, 74; *Dahi/Corrales Compagnucci*, 47 CLSR 2022, 105762, 3f; *Banasiński/Rojszczak*, 7 J. Cybersecur. 2021, 1, 5; *Hacker*, Datenprivatrecht, 294.

Designation of Roles in Personal Information Management Systems), if the approach determining the roles of each system "on a case-by-case basis" was consequently followed, a PIMS will not necessarily always take such a role.

For example, in Transparency Enhancing Technologies either providing an interpretation or an auditing of another controller's privacy policies, the PIMS will not be involved in the actual processing of personal data, making them a third party (see Part 2 Chapter 4: B. II. 1. Standardised Translations and B. II. 1. Standardised Audits). As a result, if an AI system provided the data subject with an incorrect overview of a controller's dataflow and the individual made a selection based on this information, a duty of care under the GDPR could not be established since the PIMS is neither a controller nor processor in this context. This might lead to an impossibility for the injured individual to claim any damages. If, for example, the controller's privacy policy was correct but there was an error in the interpretation caused by the PIMS, the controller would not be liable due to a lack of fault. The PIMS, on the other hand, might not be liable due to a lack of duty of care, unless such a duty could be derived from the Product Liability Directive or national tort law. Such a duty of care would however be harder to substantiate, especially if the damages were limited to the sheer violation of one's privacy preferences.

Equally problematic will be instances under which the legal qualification of the PIMS will be different for seemingly identical functionalities based on differences in the technical set-up. For example, as has been established while analysing functionalities related to the right to rectification, the PIMS may take the role of a controller or a processor (see Part 2 Chapter 4: D. II. 2. Rectification). The PIMS will be considered a controller where the platform includes the possibility of rectification at the source or has created a link between the datasets. Where on the other hand, the tool will only inform the controller about required changes through the use of push and pull notices, they will only be qualified as a processor. This technical difference in the system's functioning, which is potentially invisible to the user, will directly affect the extent of the duty of care which can be established.

Finally, the "stage-based" approach to data processing, introduced by the CJEU in *Fashion ID*,[295] leads to an outcome under which the PIMS might take different roles regarding different functionalities, as well as different stages of the overall data lifecycle. A scenario might occur under which the platform stores the user's personal data as a separate controller, verifies its identity as a processor, transfers it to another party as a joint controller, and simultaneously is considered a third party for the translation of privacy notices. Here, the data subject will run into significant difficulties in establishing which part of the process caused the damages in question and what the applicable duty of care for this stage of the processing was. In that sense, the reversal of the burden of proof for the causal link between the fault and the output only provides limited help to the data subject who is likely to run into difficulties in establishing the existence of a duty of care in the first place. This problem also again evidences that the question of which role will be taken by the PIMS is not only relevant for the determination of liability under the GDPR but stretches to other areas of the law as well.

b) Human Intervention

Another potential difficulty for data subjects in claiming damages caused by AI systems could have resulted from the restrictions provided in Recital 15 of the AILD. The Recital clarified that the presumptions established by the Directive will solely apply where the damages are caused by a fully automated output of the AI system. Instances where an AI system has only provided information or advice and a human made a subsequent decision, taking such into account, were excluded. The reasoning behind this is that in those cases, the damages should rather be traced back to a "human act or omission". This restriction directly reflects the stipulation already known from Art. 22(1) of the GDPR, where the individual's right only

---

[295]For more details refer to Part 2 Chapter 3: C. III. 3. d) f) Fragmentation CJEU, Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

applies to decisions based *"solely on automated processing"*.[296] Because of this, it would essentially be sufficient to simply have a human "confirm" the decision made by an AI system in order to avoid liability.[297] In the context of Art. 22(1), the Art. 29 WP has clarified that liability cannot be avoided by "fabricating human involvement" by such means and that the oversight over the decision would need to be meaningful.[298] The same logic should also be used in assessing to what extent a "human assessment" or "human act or omission" have led to the causation of damages where AI systems are involved.[299]

Still if the necessity for the human intervention to be "meaningful" was to be used, this could substantially affect the liability of AI-based Personal Information Management Systems. PIMS are defined as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"*.[300] As per definition, their purpose lies in ensuring that the data subject gains control of the processing operations concerning them. Based on that, it could be argued that technically the data subject would always need to be the final decision-maker, even when AI-based technologies are applied by the tool. As a result, the reversal of the burden of proof for AI providers who are also Personal Information Management Systems, would essentially have been excluded based on the

---

[296] *Hacker*, CLSR 2013, 105871, 13; *Spindler*, 11 CR 2022, 689, 700.

[297] *Wachter/Mittelstadt/Floridi*, 7 IDPL 2017, 76, 92; *Kumkar/Roth-Isigkeit*, 12 JIPITEC 2021, 289, 292; *Hacker*, CLSR 2013, 105871, 13.

[298] *Art. 29 WP*, Guidelines on Automated individual decision-making, 21.

[299] *Hacker*, CLSR 2013, 105871, 13.

[300] *EDPS*, Opinion 9/2016, para 4; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht, 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

stipulations of Recital 15. This would carry the argument *ad absurdum* but there is no denying that the general (rebuttable) presumption for any PIMS would need to be that it is the data subject who is exercising meaningful control over any decisions concerning the collection and sharing of their data. When this is combined with the previously laid down issues in establishing a duty of care, the practical applicability of the reversal of burden of proof offered by the AI Liability Directive would likely have been of little relevance when claiming damages from a PIMS provider.

3. Effect of Roles taken by the GDPR

As has been established in the preceding text, the only rules applicable to AI systems likely to effect PIMS are those concerning systems intended to interact with natural persons (see above: F. II. 1. c) aa) Systems intended to interact with natural persons). Since the transparency obligations of Art. 50(1) AIA only apply to providers, this will also be the central role in the context of PIMS. In accordance with Art. 3 No. 3, this is the entity which has developed the AI system with the intention of directly using it or putting it on the market. This role, however, does not affect the function taken with regards to the processing of personal data, nor do the obligations attached to it. The role of the provider does not automatically entail that the entity would be a data controller, processor or any other specific role under the GDPR. It rather seems that the two functions stand next to each other, with the possibility of one entity acting as both but also fulfilling either one or the other function. While the similarity of Art. 50(1) AIA to the right to information enshrined in Art. 13–15 of the GDPR might suggest some sort of interconnection, this does not seem to be the case. The two types of information (1) concerning the involvement of AI, and (2) the processing of personal data rather seem to stand next to each other. This also means that where a provider uses personal data for the development of their tool (for example, for training purposes), the obligations under Art. 13 and 14 GDPR will apply separately to the need to ensure that a user is aware of the involvement of AI (Art. 50(1) AIA). The impact of the AI Act on PIMS, therefore, does not concern the roles taken by such tools under the GDPR but

rather the extension of certain transparency obligations beyond the scope of controllership.

III. Interim Conclusions: AI-Act

The newly enacted AI Act forms part of the EU's "AI Strategy" and is intended to support the development of AI in Europe while protecting the rights and freedoms of individuals and society as a whole from risks which may arise as a consequence of these new technologies. All providers who place AI Systems on the market or put them into service in the EU are subject to the Regulation. In PIMS, natural language processing and machine learning techniques are so far only used for the provision of transparency enhancing technologies. A rise in the use of AI-based systems is, however, likely to occur especially since there are several potential options of deployment that would make the functioning of PIMI more efficient. This may, for example, involve an automated management of consent or the generation and monitoring of data subject requests. Also imaginable is the utilisation of logic- and knowledge-based approaches for the localisation, erasure, and rectification of datasets.

The involvement of AI-based technologies within a Personal Information Management System alone, however, does not automatically lead to the applicability of any obligations under the AI Act. The Act follows a risk-based approach and divides AI systems into four categories which are namely: strictly prohibited AI systems, high-risk systems, certain systems subject to transparency obligations, and all others, which are essentially left out of the scope. Since PIMS will generally not fall within the first two categories, the only obligations relevant to such are the transparency requirements established in Art. 50(1) AIA for systems intended to interact with natural persons. Based on that, the system needs to be designed and developed in a way that ensures that the individual interacting with it is aware of the AI component. This awareness should come from the sheer interaction and without the need to consult any additional notices, information sheets, terms and conditions, or any other form of communication channel.

While this requirement for transparency only relates to the utilisation of AI and not any specifics about its functioning, the obligations under 13(2)(f) and Art. 14(2)(g) of the GDPR will also apply. This means that the data subject will need to receive information about the existence of automated decision-making, including the involved logic and envisaged consequences. In contrast to the GDPR, the AI Act applies the transparency obligations to the "provider" instead of the controller. Under Art. 3 No. 3 AIA this is the party that has developed an AI system and placed it on the market or put it into service. In effect, the transparency obligations found in the GDPR are therefore extended in two ways, first, by potentially including other parties into the scope of responsibility and secondly, by extending their relevance to the development phase.

While the AI Act does not introduce any rules concerning civil liability, it provides for quite substantial fines which may be as high as €15 million or up to 3% of the PIMS' total worldwide annual turnover for the preceding financial year. Furthermore, the AI Liability Directive, which was also part of the EU's AI Strategy, was intended to alleviate certain procedural difficulties applicable to AI. This was supposed to be done through introducing certain presumptions and reversing the burden of proof in some instances. Relevant for PIMS was the presumption of causality found in Art. 4(1) AILD. Here, it was established that the causality between the fault of the defendant and the output of an AI system is to be presumed if (1) a duty of care has been violated; (2) it is reasonably likely to assume that the output has caused the identified violation; and (3) the output has caused damages on the side of the claimant.

Leading to potential problems in defining liability for Personal Information Management Systems is the establishment of a duty of care. In the context of processing personal data, the most relevant act of law in that regard is certainly GDPR. The responsibilities outlined there are, however, strictly limited to the roles of processors and controllers. Therefore, the extent to which the presumptions of the AILD may have been applied would have also depended on the role taken by the PIMS in connection to the specific functionality. Considering the inconsistencies in that regard, this might have led to substantial practical difficulties. The stipulations of Recital 15 AILD

may also have led to an ineffectiveness of the presumption introduced by Art. 4(1). The Recital establishes that the applicability of the Directive is excluded where an AI system has only provided information or advice and a human made a subsequent decision, taking such into account. It can be assumed that providers of PIMS will probably argue that the data subjects are always intended to make the final decision, with the AI only empowering them in the process.

H. Interim Conclusions: Responsibility and Liability Outside the GDPR

In addition to the applicability of the General Data Protection Regulation to Personal Information Management Systems, the effect of other laws and regulations has been analysed in the preceding section.

As a first step, the effects of the ePrivacy Directive and the Product Liability Directive were considered, both of which have been in force for a longer time but are currently being reviewed with an intention to be updated in the future. It has been established that PIMS should not be considered as an electronic communication service under Art. 3 of the ePrivacy Directive. The new draft of the ePrivacy Regulation published by the European Commission does, however, present some relevance for PIMS as Art. 9(2) explicitly recognises the possibility of using technical settings of software applications for the collection of consent. This evidences a general support for consent management functionalities and tools, the validity of which is still being questioned by certain sources. While considering the applicability of the Product Liability Directive (PLD), the main controversy centres around the question of whether PIMS could be considered a product under Art. 2 of the PLD. The extension of the current definition in order to include digital services and software is still subject to much debate. This problem is, however, solved under the new PLD, wherein software, as well as related services, will explicitly be included in the scope. The damages which could be claimed under the current PLD would either way be significantly limited in comparison to the GDPR. Under the new PLD, the two types would, however, be almost identical. Also subject to significant change are the criteria

based on which the defectiveness of a product would be determined. Here, the current PLD considers the moment at which the product was put onto the market, whereas the new Directive shifts that baseline to the point at which a product left the control of the manufacturer. As a result, PIMS would be required to upgrade and update their products as long as they can exercise control over such.

The second pillar of considered legislation comprises the Data Governance Act (DGA) and the Data Act (DA) which have recently been enacted as part of the European data strategy. The strategy aims to support the free flow of data within the market. Most relevant for PIMS is the DGA as it governs the functioning of data intermediation services. These are services that serve the explicit purpose of establishing commercial data sharing relationships between parties. Both consent management functionalities and those supporting the exercise of data subject rights will fall within that term. For transparency enhancing PIMS and storage solutions, their designation will depend on whether these are connected to a platform directed towards the establishment of such commercial relationships. Most PIMS are, however, likely to be considered data intermediation services and, based on that, will be subject to the notification procedures and conditions established within the Data Governance Act. The Act does not, however, introduce a specific regime of liability for such offerings but simply opts for a reference to national legislation and the contract between the parties instead. Of significant importance is the potential effect of the new regime on the roles taken by PIMS under the GDPR. Based on the conditions providers are subject to, it can be assumed that they will take the role of a controller for all data processing related to the intermediation itself, as well as any additional services such as storage, curation, conversion, anonymisation, and pseudonymisation. In some instances, they may still be considered as processors. The notion of the PIMS or data intermediation service being some sort of “impartial third party” completely falling outside of the scope of liability under the GDPR is, however, certainly excluded.

While not as crucial to PIMS as the Data Governance Act, the Data Act will also have some effect. Although they will not qualify as a connected service or related product, PIMS may take the role of

data holders, receiving requests for data access. This designation is, however, unlikely to have any practical significance. More relevant is their designation as data processing services as a result of which they are required to enable users to freely switch services and ensure interoperability. It can also be concluded that the Act, in a certain way, extends its impact by acknowledging the role of PIMS in supporting the overall goal of data sharing. The new obligations are imposed on businesses as other data holders additionally carry the potential for new PIMS functionalities. The Act also has some effect on the designation of roles under the GDPR, establishing that data holders always have to be data controllers, whereas a user could be both a controller and a data subject.

Another EU strategy, namely the Digital Strategy, is related to the third pillar of analysed legislation. It aims at creating a safer digital space and levelling the playing field for business. The two main regulations in this regard are the Digital Services Act (DSA) and Digital Markets Act (DMA). The applicability of the DMA to PIMS can currently be excluded. While they fall within the terminology of core platform services, there is no service provider holding sufficient market power to be considered as a gatekeeper. Most PIMS (with some exceptions) will, however, fall within the scope of the DSA as intermediary services under Art. 3(g), since the included mere conduit, caching, or hosting services are likely to form an integral part of the platform rather than just an ancillary element. As a result, they will be subject to several due diligence and transparency obligations. While the DSA does not explicitly refer to the roles taken by parties under the GDPR, the obligations put on platforms would generally suggest that they should be considered controllers under Art. 4 No. 7 GDPR. Although adding some clarity on the one hand, Recital 15 of the DSA further seems to support the fragmentation problem discussed in Part 2. It is stated here that where only certain services of a provider fall under the DSA, only those will be subject to the obligations outlined in the Act. As a result, part of a PIMS offering may be subject to those obligations and the connected presumption of controllership, while others may not.

Finally, the effect of the EU's AI strategy on PIMS has also been considered. Certain natural language processing and machine learning techniques are already applied by platform providers. The relevance of AI for PIMS is also likely to rise in the near future as there are multiple potentials for efficiently deploying such techniques. Since the AI Act follows a risk-based approach, most obligations will, however, not apply to PIMS which will fall neither within the categories of prohibited nor high-risk systems. As a result, they will only have to comply with the AI Act's transparency requirements. This means that where a system is intended to interact with natural persons, the individual needs to be made aware of the AI component. Should the PIMS fail to meet this standard, fines up to €20 million or 4% of the total worldwide annual turnover for the preceding financial year may be issued. Also of relevance may be the presumption of causality found in the draft of the AI Liability Directive. A potential hurdle in its application lies in the determination of a duty of care, which can only be established where the PIMS would be considered a controller or processor under the GDPR. Based on this, the usability of the presumptions will be largely dependent on the PIMS designation under the GDPR. This bears some risk considering both the inconsistencies as well as fragmentation established in that regard.

Chapter 7

Alternatives in the GDPR

While both relevant obligations and alternative forms of liability can be derived for Personal Information Management Systems from other EU legislation, none of the here considered laws offers a unified and comprehensive solution for all types of PIMS. Even where an applicability of the specific law was established, there is still significant differentiation depending on the specific functionalities and technical set-up of those tools. This is consistent with the findings of Part 2 of this thesis, where it has been established that depending on both technical differences and the different relationships between the parties, the level of legal responsibility assigned to providers of PIMS may vary significantly (see Part 2 Chapter 4: E. Findings for Part 2). This outcome has, however, been deemed as lacking in transparency for the data subject and essentially missing the goal of ensuring complete and effective protection of natural persons. Based on this, the possibility of alternative interpretations of the rules concerning the determination of roles taken by the parties involved in the processing of personal data under the GDPR should be considered.

The data controller is the natural or legal person who determines the means and purposes of processing of personal data (Art. 4 No. 7 GDPR). Often questionable in PIMS has been the assertion of the substantive element of determination. A party does not need to conduct the processing itself, nor do they need to have physical control

or even access to the information in order to be considered a controller. [1] They do, however, need to have the relevant decision-making power over those activities.[2] In Personal Information Management Systems, the presence of that element is not entirely clear. Is a system created for the sole purpose of empowering individuals to control the collection and sharing of their personal data able to make a relevant decision? Or are they simply an unbiased third party following the explicit orders of the user? This, after all, is argued by many providers[3] and would relieve them of any legal responsibility under the GDPR. The consideration as a processor is, on the other hand, dependent on the existence of another controller. Since it is the view presented in this thesis that this role cannot be taken by the data subject itself (see Part 2 Chapter 3: A. I. 2. b) Data Subjects), the PIMS can only be a processor where at least another entity is involved in the analysed processing activities. This leads to inconsistent results, thereby creating the question as to how decision-making power could alternatively be assumed for PIMS. The different forms from which the element of power of the processing of personal data and thereby determination can be derived have been presented in Part 2 (see Part 2 Chapter 3: A. II. 1. Determination) and should therefore be considered closely. Based on this analysis, control can either stem from a legal provision or from factual influence.[4]

---

[1] *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 7 DSGVO, para 20; Ehmann/Selmayr, *Klabunde/Horváth*, Art. 4, para 37; *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO para 18.

[2] *EDPB*, Guidelines 07/2020, para 19; *Voigt/von dem Bussche*, GDPR, 19; Sydow/Marsch / *Raschauer*, Art. 4, para 125; *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO, para 18; *Monreal*, 12 ZD 2014, 611, 612; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 7 DSGVO, para 20.

[3] Meeco´s Privacy Promise & Policy, https://media.meeco.me/public-assets/legal/meeco-privacy.pdf (accessed: 14 October 2025); Data Swift Personal Data Account (PDS) Owner Agreement, Section 7.1, https://cdn.dataswift.io/legal/hat-owner-terms-of-service.pdf (accessed: 24 October 2025).

[4] *EDPB*, Guidelines 07/2020, para 21; *Monreal*, 12 ZD 2014, 611, 612.

A. Legal Provision

In accordance with Art. 4 No. 7 GDPR, the controller and the specific criteria for their nomination may be specified by European Union or Member State law, where this law determines the means and purposes of the processing of personal data. A legal act may therefore explicitly designate a specific entity as a data controller.[5]

I. In EU Law

Such designations have in fact been identified in some of the legal acts considered in this thesis.[6] The Data Act explicitly mentions the respective designations under the GDPR in multiple Recitals. The exclusion of data processors from being data holders can, however, not be understood as designating all data holders as controllers, but rather the other way around. Where an entity holding data is not a data controller at the same time, the obligations under the DA should not apply. The same can be said about the content of Recital 34 which establishes that users may take the role of both the data subject and the controller. Also, partially excluding the possibility that the DA would significantly affect the roles under the GDPR is Art. 1(5), which establishes that in the case of conflict between the two laws, the GDPR should prevail.

Potentially establishing a form of controllership are, however, the Data Governance Act[7] and the Digital Services Act.[8] The provision of both data intermediation services (Art. 2(11) DGA) and intermediary services (Art. 3(g) DSA) is subject to several conditions and obligations which require both the processing of personal data and some level of control over the processing operations. For example,

---

[5] *EDPB*, Guidelines 07/2020, para 23; *Monreal*, 12 ZD 2014, 611, 612; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 7 DSGVO, para 23.

[6] See Part 3 Chapter 6: C. II. 6. Effect on Roles taken under the GDPR; D. IV. Effect on Roles taken under the GDPR and E. II. 4. Effect on Roles taken under the GDPR.

[7] See Part 3 Chapter 6: C. II. 6. Effect on Roles taken under the GDPR.

[8] See Part 3 Chapter 6: E. II. 4. Effect on Roles taken under the GDPR.

Art. 12(c) DGA only allows for data generated about the user as a part of such service, to be used for its further development. Art. 12(e) DGA allows for services to be provided for purposes such as facilitating the exchange of data, temporary storage, and curation. Art. 12(o) DGA asks for the maintenance of a log record of the data intermediation activity and Art. 12(d) DGA for the conversion of data formats to ensure interoperability. Similarly, intermediary services must create notification mechanisms for illegal content (Art. 16(1) DSA); decide on restrictions imposed on the use of the service (Art. 14(1) DSA); and generate reports on content moderation (Art. 15(1) DSA). For all of those actions, the law has established a purpose and designated an entity who is responsible for its fulfilment. Where a task of a duty is being imposed on a legal entity in such a form, they will be considered as data controller with control stemming from the legal provision.[9]

While an implied legal designation of controllership should be assumed in those instances, it unfortunately does not constitute a comprehensive designation applicable to all PIMS. It has also been established in the preceding pages that not all types of PIMS service offerings fall within the scope of data intermediation (Art. 2(11) DGA) and intermediary services (Art. 3(g) DSA). While these legal acts may therefore effectively substantiate an element of control and therefore "determination" in the meaning of Art. 4 No. 7 GDPR, this will only apply to the extent that the service offering falls within their scope. In fact, the idea of "fragmentation" of processing activities introduced by the CJEU Case Law[10] is in a sense supported by Recital 15 of the DGA, which specifies that where some services of one provider fall within the scope of the Act and others not, the relevant provisions will only apply to the first. In that sense, the question may be asked whether the enactment of a specific law regulating PIMS

---

[9]*EDPB*, Guidelines 07/2020, para 24; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 7 DSGVO, para 24f.

[10]Part 2 Chapter 3: C. III. 3. d) f) Fragmentation; Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 84.

should be considered in order to ensure a more consistent determination of roles. This possibility will be subsequently discussed under D. Interim Conclusions: Alternatives in the GDPR and Necessity for New Regulations.

II. In Nationale Legislation

At least briefly mentioned in this context should be § 26 of the German TDDDG and the new "Consent Management Regulation" (Einwilligungsverwaltungsverordnung – EinwV), which has been enacted on September 2024.[11] While this thesis is focused on EU-wide legislation and not national peculiarities, this regulation is quite significant as it is the first time that Member State law has attempted to explicitly regulate PIMS.[12] Including such was in fact subject to many controversies before its enactment, with the paragraph essentially being added in the final stages.[13] At the time of writing, many aspects such as the general permissibility of managing consent through platforms,[14] the position of the provider,[15] and the relation of the TDDDG to the Data Governance Act,[16] as well as the intended ePrivacy Regulation,[17] were being heavily debated. Interesting in this context is, however, to what extent controllership (or another role) could be derived from the provided stipulations.

§ 26(1) of the TDDDG states that consent management services need to (1) establish a user-friendly and competitive procedure for the collection and management of consent; (2) be free of any own

---

[11]BT-Drs 20/12718, Verordnung nach § 26 Absatz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und zur Änderung der Besonderen Gebührenverordnung Telekommunikation (4 September 2024).

[12]*Kühling/Sauerborn*, 10 ZD 2022, 531, 532.

[13]Assion / *Aretz*, § 26 TTDSG, para 9-14.

[14]ibid para 17.

[15]*Kühling/Sauerborn*, 10 ZD 2022, 531, 533 Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 37-41.

[16]Gierschmann/Baumgartner / *Hanloser*, § 26, para 12f; Assion / *Aretz*, § 26 TTDSG, para 19f.

[17]Gierschmann/Baumgartner / *Hanloser*, § 26, para 14f Assion / *Aretz*, § 26 TTDSG, para 15f.

commercial interests in the provision of consent and be independent from any parties, which might have such; (3) process personal data, only for the purpose of managing the individual's consent; and (4) submit a security concept allowing an assessment of the quality and reliability of the service. Where a provider meets these requirements, they may be recognised by an independent body (§ 26(1) TDDDG). The specifics of both the actual recognition procedure and more detailed requirements concerning the service's technical and organisational measures are determined the new "Consent Management Regulation" (Einwilligungsverwaltungsverordnung – EinwV).[18] On their own, these specifications may, however, provide sufficient grounds for defining a role of such a provider under the GDPR.

The section directly establishes the allowed purposes of the processing of personal data within the platform.[19] These are limited to only the management of consent, and any alternative interests, commercial or otherwise, are explicitly excluded. It also refers to the determination of means in the form of submitting a security concept. In that sense, the TDDDG seems to clearly designate the provider of such a consent management platform as a data controller.[20] This designation only covers the processing within the platform and not the further activities of the end-controller who receives the data as a result of the provided consent.[21] While the legal designation of controllership is not explicitly mentioned in this context, it seems to be the only logical outcome, especially since the possibility of a platform taking the roles of a data processor is directly excluded in § 26(1) No. 2 TDDDG, which stipulates that they need to be independent from other parties having a commercial interest in the data.[22] It

---

[18]BT-Drs 20/12718, Verordnung nach § 26 Absatz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und zur Änderung der Besonderen Gebührenverordnung Telekommunikation (4 September 2024).

[19]Assion / *Aretz*, § 26 TTDSG, para 47; Geppert/Schütz / *Schmitz*, TTDSG §26, para 21; Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 25.

[20]Riechert/Wilmer / *Golland/Riechert*, § 26 TTDSG, para 20.

[21]ibid para 12.

[22]Assion / *Aretz*, § 26 TTDSG, para 45.

should, however, be noted that this solely relates to the type of platforms established in § 26 TDDDG and not any other types of PIMS.

B. Factual Influence

When control cannot be derived from any sort of legal designation, whether explicit or implicit, the factual circumstances of the processing need to be analysed.[23] Such an assessment, based on the actual roles taken by those tools, has already been conducted in Part 2 of this thesis (see: Part 2 Chapter 4: Designation of Roles in Personal Information Management Systems) and should therefore not be repeated here. What may, however, be considered are alternative forms of interpretation based on notions applied in other contexts.

I. Relationship of Trust

It has been established both within academic literature as well as by relevant authorities that there are certain roles or professions which, based on established practice, will always have to take the role of data controller.[24] Textbook examples include professions such as lawyers, doctors, or accountants.[25] Here controllership is presumed based on the fact that these occupations are highly regulated and individuals are subject to many rules such as codes of conduct or ethical guidelines, as well as professional secrecy.[26] In that sense, they need to act fully independently and cannot be bound by instructions, excluding the possibility of being considered a processor under Art. 4 No. 8.[27]

---

[23] *EDPB*, Guidelines 07/2020, para 25; *Bassini*, BLP 2019, 103, 109; *Monreal*, 12 ZD 2014, 611, 612.

[24] *Monreal*, 12 ZD 2014, 611, 612; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13; *EDPB*, Guidelines 07/2020, para 27.

[25] *DSK,* Kurzpapier Nr. 13, 4; Gola/Heckmann / *Gola*, Art. 4 DSGVO, para 85; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13.

[26] *DSK,* Kurzpapier Nr. 13, 4; *Radtke*, Gemeinsame Verantwortlichkeit, 140.

[27] *EDPB*, Guidelines 07/2020, para 80; Kühling/Buchner / *Hartung*, Art. 4 Nr. 7 DSGVO, para 13.

Another reason for automatically assuming controllership for certain roles is the presence of a certain responsibility towards the data subject. This will certainly apply to the professions listed previously, where an individual goes to one of the parties precisely for the purpose of receiving support in a matter which they cannot handle on their own.[28] Another textbook example of controllership deriving from the proximity between the parties, is that of an employer to an employee.[29] Here it is generally accepted that an employer will always need to act as a controller for data concerning their employees.[30] This assumption can be based on multiple reasons. First, an employer typically assumes a certain extent of responsibility for their employees, especially since the employee will probably act based on their employer's instructions.[31] Second, the employee can be seen as a particularly vulnerable party, since they depend on their employer.[32] Finally, this leads to the fact that there needs to be a certain level of trust between those two parties, thereby in a sense binding them together and making them responsible for one another.[33] The unique character of this relationship is also indirectly recognised through Art. 88 of the GDPR which allows Member States to provide more specific rules for the assurance of the rights and freedoms of employees in the context of the processing of their personal data. In effect, the notion that the employer could shift the controllership and thereby responsibilities for their employees onto other parties would be highly undesirable.

---

[28] *Radtke*, Gemeinsame Verantwortlichkeit, 40; Sydow/Marsch / *Ingold*, Art. 28, para 15; Kühling/Buchner / *Hartung*, Art. 28 DSGVO, para 41.

[29] *Monreal*, 12 ZD 2014, 611, 612; *Lücke*, 10 NZA 2019, 658, 660.

[30] *Monreal*, 12 ZD 2014, 611, 612; Wolff/Brink/v. Ungern-Sternberg / *Schild*, Art. 4 DSGVO, para 93h; *Lücke*, 10 NZA 2019, 658, 660; *Jung/Hansch*, 4 ZD 2019, 143, 146; *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 89.

[31] *Richter*, 24 ArbRAktuell 2020, 613, 614; *Körner*, 16 NZA 2021, 1137, 1140.

[32] *Art. 29 WP*, Guidelines on DPIA, 10; *Düwell/Brink*, 17 NZA 2023, 1097, 1098; *Körner*, 16 NZA 2021, 1137, 1138.

[33] *Bassini*, BLP 2019, 103, 109; *Weichert*, 1 NZA 2023, 13, 19.

In the view presented here, the same reasoning can apply to Personal Information Management Systems. PIMS should empower individuals to take control over the processing of their personal data. This need to take control leads back to feelings of helplessness and a perceived power imbalance between businesses and individual users reported by data subjects.[34] Many admit that they feel confused by current processing practices and are not sure how their data is being used.[35] The typical user of a PIMS is therefore likely to be a data subject who feels that they are unable to take control of the processing operations concerning themselves. They turn to a tool which promises to ease this problem by supporting them and mitigating existing power imbalances. Similarly in regard to consulting a doctor, tax consultant, or lawyers, this individual is therefore actively looking for help in a matter which they cannot resolve because of a lack of expert knowledge. Furthermore, they can be considered as being in a vulnerable position; they feel a lack of control and power over in the current situation. Finally, they presumably enter into a relationship of trust with the PIMS. This tool is supposed to help them, support them, and act on their behalf. It is clearly implied here that the PIMS is seen as a form of "protector" of the individual's personal data on their behalf. This expectation is also by no means unreasonable looking at examples of how PIMS market themselves. Promises such as equipping *"individuals with tools to collect, store, use and share their data to manage their lives better",*[36] pursuing a *"mission of empowering individuals with their data"*,[37] or empowering *"users to protect their online choices in a human-centric, easy and enforceable*

---

[34]*Christl*, Corporate Surveillance 31, 85; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *EDPS*, Opinion 9/2016, para 4.

[35]*Clifford/Graef/Valcke*, 20 GLJ 2019, 679, 685ff; *Soh,* 5 EDPL 2019, 65, 65f.

[36]MyDex, https://mydex.org/ (accessed 15 October 2025).

[37]ibid.

manner",[38] are the rules rather than the exceptions. In turn, an expectation is created that this tool will support and actively protect the individual's privacy.

This leads to the formation of a relationship of trust and in a sense, dependence on the tool. Based on that, a clear analogy can be drawn between the offering of a Personal Information Management System and services provided by lawyers, consultants, doctors or other type of advisors. A similar notion has in fact already been proposed by Jack M. Balkin, who argued that digital companies processing personal data should be regarded as "information fiduciaries" due to the vulnerability and dependence of individuals created by information capitalism.[39] Furthermore, this trust, vulnerability and dependency on the PIMS clearly evidences similarities with the employee-employer relationship. It is therefore the view presented here that PIMS should in the same manner be in principle qualified as data controllers in relation to all processing activities concerning their users, regardless of any technical or contractual specifications.

II. Expectation of the Data Subject

Closely related to the relationship of trust formed between a provider of a Personal Information Management System and the data subject is another factor which may be taken into account when determining the roles taken by a specific party. This is the perspective of the data subject.[40] While certainly not the most decisive element, the notion of considering the subjective viewpoint of the affected individual, while determining the level of responsibility of the parties, is generally supported.[41] This results directly from the principle of trans-

---

[38]Advanced Data Protection Control, https://www.dataprotectioncontrol.org/ (accessed: 15 October 2025).

[39] *Balkin*, 133 HARV. L. REV F. 2020, 11, 11.

[40] Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 149; *Radtke*, Gemeinsame Verantwortlichkeit, 114.

[41]Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 149; *Radtke*, Gemeinsame Verantwortlichkeit, 114.

parency enshrined in Article 5(1)(a) GDPR, which states that personal data should be processed lawfully, fairly and in a transparent manner. Since all relevant elements of the processing, including the responsible parties, should be transparent to the individual, leaving them with a false impression should naturally be attached to legal consequences. After all, the GDPR puts much emphasis on the creation of user-friendly and understandable privacy notices, clearly opposed to practices such as creating lengthy, complicated texts, [42] hiding information in general terms and conditions,[43] or spreading information throughout different channels.[44] In the case of Personal Information Management Systems, the overall circumstances are likely to create an impression for the data subject that the provider is actively managing and thereby controlling their dataflows on their behalf. This entity is their primary counterpart. Thereby a reasonable expectation is formed that this is also the entity responsible for those processing activities. The requirement of intelligibility also encompasses the need to take the level of knowledge of the target audience into account.[45] An individual looking for support from the PIMS will likely do so in order to receive assistance in the protection of their data, based on a lack of understanding in the matter or time to deal with the relevant questions. The individual may in fact not be aware of the exact definition of "controller" and the various prerequisites and legal interpretations surrounding that term. From their subjective perspective, the assumption that the Personal Information Management System is therefore the primarily responsible entity under the GDPR would thereby be entirely logical.

The notion of giving legal relevance to the data subject's "reasonable expectations" is also directly supported in Recital 47 in the con-

---

[42] Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 12; Sydow/Marsch / *Greve*, Art. 12, para 14.

[43] *Art. 29 WP*, Guidelines on transparency, para 8.

[44] *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, para 521f.

[45] *Art. 29 WP*, Guidelines on transparency, para 9; Rücker/Kugler, *Schrey*, D. General conditions, para 606; Ehmann/Selmayr, *Heckmann/Pascke*, Art. 12, para 13.

text of using legitimate interest as a legal basis for processing personal data. Here it is stated that the determination of whether the rights and freedoms of the individual are overriding the interests of the controller needs to take into consideration *"the reasonable expectations of the data subject based on their relationship with the controller"*, as well as what *"a data subject can reasonably expect at the time and in the context of the collection of personal data"*. The idea of considering the individual's perspective is also supported by the general objective of ensuring *"effective and complete protection"* solidified by CJEU Case Law.[46] After all, should the data subject be left in a situation where they are unsure who to contact regarding the exercising of their rights or from whom to claim damages, this would directly go against this notion. The overall impression given to them, as well as their interpretation of the circumstances therefore needs to be adequately accounted for, in order to avoid any gaps or shortcomings in protection. When combining this element with the previously identified relationship of trust potentially formed between the data subject and the Personal Information Management System, an apparent need for controllership on the side of the PIMS, independently from any other actors, emerges.

III. Transfer of Decision-Making Power

Another consideration is to what extent it is possible for the data subject to transfer their decision-making power onto the Personal Information Management System. As has been discussed under Part 2 Chapter 3: A. I. 2. b) Data Subjects, data subjects do to a large extent determine the means and purposes of the processing of their own personal data, raising the question whether they may also be

---

[46]Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 34; Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 28; Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551, para 66; Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 66.

considered as a data controller.[47] This notion has been rejected based on the fact that this would essentially offset a number of relevant protections given to individuals under the GDPR, thereby going against the intention of the law.[48] Still the fact that the data subject is in a sense arguably the main actor responsible for the determination of the purposes and means of processing of their data cannot be denied

In order to be considered a controller, a party needs to have relevant decision-making power over the processing of personal data. [49] As has, however, been established in Part 2 of this thesis (see Part 2 Chapter 4: E. Findings for Part 2), the presence of this element of determination cannot always be confirmed for Personal Information Management Systems. For example, in consent management, a PIMS will be considered a third party regarding the intended end processing activity for which the consent is being provided (see Part 2 Chapter 4: C. II. 1. a) Intended Activity). Similarly, they will likely qualify as a processor when supporting the exercising of the right to rectification in the form of push and pull notices (see Part 2 Chapter 4: D. II. 2. c) aa) Automated Notifications Requested by the Controller). This is largely based on the fact that the PIMS will not have any relevant decision-making power concerning the processing activity as they are arguably only acting based on the user's instructions.[50]

It could, however, be argued that the data subject, by selecting and using the PIMS, is essentially transferring their own decision-

---

[47] *Wagner*, 7 ZD 2018, 307, 307; Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Finck*, Blockchain Regulation, 101; *Edwards and others*, IPR 2019; *Peitz*, Verantwortlichkeit in Blockchain, 212; *Finck*, 11 IDPL 2021, 3333, 338.

[48] Kuner and others / *Bygrave/Tosoni*, Art. 4(7), 145, 154; *Finck*, 11 IDPL 2021, 333, 343; *Edwards and others*, IPR 2019.

[49] *EDPB*, Guidelines 07/2020, para 19; *Voigt/von dem Bussche*, GDPR, 19; Sydow/Marsch / *Raschauer*, Art. 4, para 123; *Spindler/Dalby* / Spindler/Schuster, Art. 4 DS-GVO, para 18; *Monreal*, 12 ZD 2014, 611, 612; *Petri* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 4 Nr. 7 DSGVO, para 20.

[50] https://media.meeco.me/public-assets/legal/meeco-privacy.pdf (accessed: 14 April 2026); https://cdn.dataswift.io/legal/hat-owner-terms-of-service.pdf (accessed: 14 April 2026).

making power onto the provider. After all, Personal Information Management Systems are intended to support the individual in the exercising of their rights, thereby acting in the form of an "extended arm" of that individual. If, for example, the user sets up certain generalised consent preferences or interests in data removal, they will at the same time empower the tool to exercise control on their behalf. Where the element of determination for the means and purposes will therefore not lie directly with the PIMS, it will be indirectly derived from the data subject. Based on the assumption applied in this thesis (see Part 2 Chapter 3: A. I. 2. b) Data Subjects) that the data subject cannot be a controller for their own personal data, the PIMS will inadvertently take that role through the determined transfer of decision-making power. This will also apply regardless of the level of such. Even where the PIMS is only acting "on behalf of" the data subject and strictly following the individual's order, they will still take the role of a data controller.

IV. Enabling Data Transfers

In the case of *Fashion ID*, the CJEU established the origins of the necessary element of determination of means and purposes from an entirely new element, namely the fact that the company *"made it possible for Facebook Ireland to obtain personal data"*.[51] The Court argued that since without the inclusion of the plug-in, the data transfer would not have occurred, the website operator is in fact exerting *"decisive influence over the collection and transmission of the personal data"*.[52] As a result, while not responsible for any subsequent processing of personal data conducted by Facebook, a joint controllership over the *"the collection and disclosure by transmission of the personal data of visitors to its website"* was established.[53]

An analogy could be drawn from this for Personal Information Management Systems. Their primary goal is empowering individuals

---

[51]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 75.
[52]ibid para 78.
[53]ibid para 76.

in the exercising of their rights. [54] Other goals such as incentivising more data sharing and supporting the creation of new application and business models based on that are, however, also frequently mentioned.[55] The idea behind this is that the enhanced control which data subjects are given over their dataflows will also lead to more trust on their side and result in more willingness to share their data within the EU, while at the same time keeping high standards for data protection.[56] PIMS may therefore be considered as also serving the purpose of enabling the collection and transmission of personal data in order to support the overall growth of the EU data economy. Based on this, they would need to be qualified as a data controller in the same vein as has been established for website operators in the case of *Fashion ID*.

---

[54] *EDPS*, Opinion 9/2016, para 4; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 2; *Riechert/Richter*, Was die DSGVO braucht, 8; https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026); https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (accessed: 25 Februar 2026).

[55] *EDPS*, Opinion 9/2016, para 6; *European Commission*, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016), 11; Mydex, 'Achieving Transformation at Scale', https://mydex.org/resources/papers/AchievingTransformationAtScale/AchievingTransformationatScaleMydexCIC-2021-04-14.pdf (accessed: 24 October 2024), 2; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

[56] *Janssen/Cobbe/Singh*, 9 IPR 2020, 1, 7; https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1 (accessed: 12 October 2024); https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy (accessed: 25 February 2026).

This will particularly be relevant in consent management related functionalities, since here the goal of "enabling data transfers" is particularly evident. However, the same notion could also be extended to transparency enhancing technologies. Technically, interpretative tools will typically only provide the user with an overview of possible processing activities conducted by other parties and not process any personal data by themselves.[57] If, however, the interpretative functionality was linked to consent management it could be considered as serving the same overall purpose, namely enabling the transfer to another entity. After all, should certain facts or statements made by the data recipient be misinterpreted by the PIMS and thereby be incorrectly presented to the data subject, they could potentially approve a specific transfer based on false facts. Here the PIMS would actively contribute and essentially make possible a data transfer which might not even be in line with the individual's preferences and at the same time, not be the responsibility of the data recipient. The reason for this incorrect transfer will also not relate to the consent management functionality, but more so to the interpretative function, meaning that it was this specific part of the service which enabled the data transfer without the processing of any actual personal data.

In the context of functionalities focused on the facilitation of data subject rights, the right to portability will very clearly also serve the purpose of enabling data transfers. On the other hand, the right to erasure and objection obviously are directly at the completely opposite goal. In a sense, however, the exercise of these rights can also be viewed as a type of "re-transfer" of data. From a practical perspective, the individual will probably still be in possession of the same information, therefore making the transmission of such from a controller back to the individual unnecessary. Still, ordering the removal of a previously submitted dataset can be viewed as a form of return of data, into the sphere of control of the individual and therefore in a sense a "transfer". Even more so in the context of the right to access, where the receipt of a copy very clearly constitutes a transfer and while receiving information about a processing activity

---

[57] See Part 2 Chapter 4: B. I. Interpretative.

cannot technically be equated to a "data transfer", it does serve the overall purpose of understanding what type of information the controller possesses and potentially initiating a transfer based on such. PIMS can therefore certainly be considered as serving the purpose of "enabling data transfers" for which they should consequently be considered controllers based on the CJEU case law.

C. Limitation of Fragmentation

As has already been established in Part 1 of this thesis, the introduction of the stage-based approach to data processing operations and the fragmentation of processing activities connected to such by the CJEU has been subject to much criticism.[58] The artificial splitting of the overall chain of processing can significantly impede transparent communication and lead to a lot of confusion on the side of the individual data subject.[59] It may also result in quite significant legal uncertainty with regard to the division of responsibilities for each separate phase.[60] This effect has also been observed in the context of Personal Information Management Systems, where, as a result, different roles would be taken by the service provider for different functionalities.[61] Since the decisions and interpretations of the CJEU are, however, legally binding, they need to be applied regardless of any potential criticism. What may, however, be considered is an extension, or rather a limitation of certain concepts, as long as it does not go against the reasoning of the court's findings.

The Court of Justice of the European Union has over and over again supported the notion that the GDPR should be interpreted in a way, which ensures the *"effective and complete protection"* of the

---

[58]See Part 2 Chapter 3: C. III. 3. d) ff) Fragmentation.

[59]*Paun*, 9 EuCML 2020, 35, 37; *Zalnieriute/Churches*, 83 MLR 2020, 861, 871-874; https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026).

[60]https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1 (accessed 25 February 2026); *Mahieu/van Hoboken/Asghari*, 10 JIPITEC 2019, 85, 96.

[61]See Part 2 Chapter 4: E. Findings for Part 2.

data subject.[62] The interpretation in accordance with the *effet utile* and thereby the purpose of the provision is, after all, a form of interpretation frequently applied by the CJEU.[63] It can also be confirmed that in the case of *Fashion ID*, the introduction of the stage-based approach did lead to a more comprehensive regime of protection, since the website operator was included in the scope of controllership. As has, however, been evidenced in this thesis, there are instances—one of those being Personal Information Management Systems—where the application of this approach leads to the opposite results. Instead of extending the level of responsibility on the side of the PIMS, the splitting of the various platform functionalities will often result in a lack of responsibility for certain parts of the platform or activities outside of such.[64] This not only limits the scope of responsible parties but effectively further hinders the individual from truly understanding the extent of the platform's involvement and the connected legal implications. Such a result is particularly unacceptable in instances where the entire purpose of the service offering supposedly lies in supporting the individual user in the exercise of their rights. This form of interpretation thereby is most definitely not in line with the *effet utile* of the GDPR, nor in fact the purpose of PIMS. Based on this analysis, an expansion of the interpretation should be considered.

In accordance with Article 4 Nr. 2 GDPR, processing means *"any operation or set of operations which is performed on personal data or on sets of personal data".* It may therefore refer to both a singular activity, as well as a number of connected steps.[65] This closely re-

---

[62]Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 34; Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, para 28; Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551, para 66; Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 66.

[63]*Bergmann*, 'Effet utile' in HdLexEU; *Potacs,* 44 EuR 2001, 465, 465; *Sadl*, 8 EJLS 2015, 18, 22; *Fennelly*, 20 Fordham Int'l L.J. 1996, 656, 674.

[64]See Part 2 Chapter 4: E. Findings for Part 2.

[65]Rücker/Kugler, *Rücker*, B. Scope of application, para 53.

lates to the term of “processing activity” which is never formally defined within the GDPR but is still frequently used.[66] As has been discussed in Part 2 of this thesis (see Part 2 Chapter 3: A. II. 3. Processing), this mostly refers to instances where multiple “processing” steps are bundled into one “activity” which serves the same purpose and should therefore be considered as one overall action.[67] For example, handling job applications will typically be considered as one “activity” rather than separated into the isolated actions of collecting CVs, reviewing them, contacting applicants, interviewing them etc. This type of consolidation is after all quite relevant and in fact necessary when creating a record of processing activities, as it would otherwise likely result in an unmanageable amount of entries.[68] The idea that processing can thereby relate to one action, as well as a number of consecutive but still connected operations is clearly supported in data protection law.[69]

Based on that notion, it is the view presented here that where it serves the purpose of ensuring effective and complete protection for the data subject, a rule of unification rather than fragmentation should be applied when determining the roles and responsibilities of the parties involved in the processing of personal data. This rule of unification should apply especially to instances under which a chain of activities serves one overall purpose and appears as one consolidated action to the data subject. This will be the case for Personal Information Management Systems, as well as any other type of interactive platforms. Here, the user signing up to these clearly makes a decision to use a specific service and not a separate resolution for each of the elements of such. A job applicant applying for a job is informed and agrees to the overall processing of their personal data

---

[66]See Articles: 3 (2); 4 Nr. 16 b); 24 (2); 28 (4); 30; 35 (6) and (10); 40 (6) and (7); 42 (6) and 60 (10), as well as Recitals: 3; 19; 23; 24; 32; 36; 63; 74; 80; 81; 84; 93; 94; 104; 115; 126 and 131.

[67]Paal/Pauly / *Martini*, Art. 30 DSGVO, para 5; Ehmann/Selmayr / *Bertermann*, Art. 30, para 8; Kühling/Buchner / *Hartung*, Art. 30 DSGVO, para 15.

[68]*Roßnagel* / Simitis/Hornung/Spiecker gen. Döhmann, Art. 30 Nr. 2 DSGVO, para 16.

[69]Rücker/Kugler, *Rücker*, B. Scope of application, para 53.

for the purpose of reviewing their application. This involves all the relevant steps from submitting the CV, it being assessed, and the data being captured in a system, to deciding who to invite for interviews and sending out invites, etc. The individual does not see all of these as separate activities and no controller would ever communicate them in that way. The same goes for signing up onto a platform like a PIMS. A data subject wishes to manage the entirety (or part) of their personal data flows through the provider. Functionalities such as providing an overview of processing activities, allowing data access and portability, submitting erasure requests, and storing data and transferring it to other controllers based on consent are viewed as one overall control mechanism and not separate actions. Based on that, they should also be categorised as one "processing activity".

Such a unification, while intuitively constituting the opposite of the fragmentation introduced by the CJEU, also does not in fact negate this approach. The fragmentation was introduced in order to separate the activities connected to Facebook (data transfer through the embedded plug-in) from those unrelated to them (overall website management).[70] It also served the purpose of exempting Fashion ID from any responsibility for subsequent data processing conducted by Facebook outside their scope of control.[71] This division could still be maintained where parties other than the data subject and the PIMS are involved. For consent management or data portability related functionalities, the assumption of joint controllership is still possible where a joint determination of means and purposes takes place. Likewise, the PIMS would naturally not be considered a controller for any processing activities conducted outside of the platform's control. Should, for example, an end controller further process personal data for purposes other than those determined in the transfer, based on Art. 6(1)(f) this would naturally be done in sole controllership of that entity.

The idea of unification only extends to the platform itself but includes any activities managed directly within in the platform, as well

---

[70]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 83.
[71]Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 76.

as based on its actions. As a result, activities technically conducted as third parties or processors so far would be included in the unified scope of controllership. For example, transparency enhancing service offerings[72] would not be reviewed separately but rather in unity with the other platform elements (such as the management of consent or data subject requests), meaning that they would now take legal responsibility under the GDPR for those activities as well. The same goes for functionalities related to the identification of the data subject or a link between the individual and the dataset.[73] Similarly, functionalities for which previously various roles could be taken depending on their specific technical set-up, should also be considered uniformly as part of the platform. For example, in the context of the exercising the right to erasure, the PIMS could potentially take any roles under the GDPR for revocation-related functionalities.[74] It was concluded there that while the platform would be considered a data controller for the assignment of a unique identifier and the encryption of a dataset, they would also be considered a processor where the platform was cooperating with the business users. This possibility is now excluded based on the principle of unification, as the PIMS would be forced into the roles of controller for the platform overall, regardless of any specific technical differences or diverging agreements with other entities.

Such a unification could be seen as quite a burden for the PIMS provider who would now essentially be unable to transfer any sort of responsibility onto the other involved parties. It is, however, the view presented here that this outcome would still be the fairest, considering the circumstances. The notion that a Personal Information Management System only acts “on behalf” of the data subject and in accordance with their wishes and thereby should be excluded from responsibility under the GDPR, often argued by platform providers, [75]

---

[72]See Part 2 Chapter 4: B. Information.

[73]See Part 2 Chapter 4: D. I. 2. Identification.

[74]See Part 2 Chapter 4: D. II. 3. e) Revocation.

[75]Meeco’s Privacy Promise & Policy, https://media.meeco.me/public-assets/legal/meeco-privacy.pdf (accessed: 24 October 2025), 6; Data Swift Personal Data

is not supported here. Users selecting to manage their data through a specialised platform rather than on their own, are likely to do so precisely due to a lack of own expertise. As has been established previously in this thesis, the creation of a relationship of trust can be assumed and avoiding responsibility in such a scenario would lead to an unfair result.

Arguably, the transfer of responsibility onto other data controllers would be less harmful. The assumption of unified controllership over all involved processing activities of the PIMS might result in the fact that any claims for damages by data subjects will now be made against the platform. Since Art. 82(4) establishes a regime of joint and several liability for instances where multiple parties are involved, any controller can be held liable for the entire damages, regardless of their actual involvement.[76] It is therefore possible that PIMS providers might be held liable for damages caused by other controllers. Art. 82(5) GDPR allows the indemnification for such damages corresponding to the level of responsibility each of the parties bears regarding the infringement. Still, re-claiming already paid compensation can be viewed as an additional burden for the PIMS. It is, however, the view presented here that such a burden is proportionate considering the circumstances. The intention of Personal Information Management Systems lies in the support of individuals in the exercise of their rights. This arguably includes the right to receive compensation for any damages incurred as a result of a processing activity. In that sense "standing in" for the damages of other controllers could be viewed as an additional element of the overall service offering. Also, extending the responsibility of the platform over the typical level of responsibility held by other controllers is justifiable considering that these services are explicitly being marketed as ensuring privacy friendly solutions. Where data transfers are facilitated through

---

Account (PDS) Owner Agreement Section 2.1.(b), https://cdn.dataswift.io/legal/hat-owner-terms-of-service.pdf (accessed: 24 October 2025).

[76]Kuner and others / *Zanfir-Fortuna*, Art. 82, 1160, 1176; *Wybitul/Neu/Strauch*, 5 ZD 2018, 202, 204; *Paal*, 1 MMR 2020, 14, 18; *Kohn*, 11 ZD 2019, 498, 501; Ehmann/Selmayr / *Nemitz*, Art. 82, para 58; Rücker/Kugler, *Schumacher*, D. General conditions, para 831.

the platform, the data subject will naturally be inclined to feel a higher level of security than when sanctioning such themselves. The risk of the PIMS of assuming liability for certain subsequent actions outside of their scope of control is therefore a direct reflection of this impact. It is not unreasonable for a data subject to expect certain assurances from a service provider promising the protection of their rights. In that sense, while there may be scenarios under which a PIMS might need to take responsibility without any fault on their side, the overall circumstances do justify those exceptions, as leading to the overall most fair result.

D. Interim Conclusions: Alternatives in the GDPR and Necessity for New Regulations

Alternative forms of interpretation within the GDPR have been considered, since the previous interpretations and alternative forms of deriving liability have not led to satisfactory results. The legal acts analysed in Chapter 6: Liability outside of the GDPR do not allow for uniform controllership to be derived from union law. The same goes for the analysed national legislation, namely the German Telecommunications Digital Services Data Protection Act and the connected draft of the "Consent Management Regulation" (Einwilligungsverwaltungsverordnung—EinwV). While the provisions found there would likely allow for controllership to be derived from legal designation, this only covers the type of platforms established in § 26 TDDDG and not any other PIMS functionalities.

There is, however, the possibility of deriving controllership from factual influence, based on certain special characteristics of personal Information Management Systems. First, an analogy can be drawn to professions such as lawyers, doctors, or accountants, as well as the relationship between an employer and employee. Here controllership is always assumed based on the specific relationship of trust required between the parties. Users of PIMS are likely to select a tool as they feel a need for support. This puts them in a vulnerable position and creates a relationship of trust between the parties. As a result, the PIMS should be qualified as data controllers in the same

manner as is established for other types of services. Based on the principle of transparency, the perspective of the individual users should also be considered. Personal Information Management Systems will often create the impression of actively managing and thereby controlling their dataflows on the individual's behalf, creating a reasonable expectation on the side of the individual users that they would also take responsibility for such. It could also be argued that where the element of determination for the means and purposes will not lie directly with the PIMS, it will be indirectly derived from the data subject, who essentially transfers their own decision-making power onto the provider. Finally, based on CJEU case law, the element of determination could also be assumed on the basis that Personal Information Management Systems exert a decisive influence over the processing of personal data, by enabling data transfers both to and from other controllers.

Another suggested solution concerns the expansion of the stage-based-approach in line with the *effet utile* of the GDPR. The term processing refers to *"any operation or set of operations"* and can therefore relate to both a singular activity, as well as a number of connected steps. The GDPR therefore allows for both the fragmentation and the unification of various processing activities conducted for the same purpose. While, therefore, the division into various stages conducted by the CJEU in order to ensure effective and complete protection was absolutely valid, the exact opposite may also be done to achieve the same effect. Based on that, a rule of unification is suggested for instances under which a chain of activities serves one overall purpose and appears as one consolidated action to the data subject. As a result, all activities performed by the PIMS platform should be subsumed as one chain of processing for which a uniform role, namely that of a data controller, needs to be assigned. While this assumption might create some additional burdens for PIMS providers who could be held responsible for processing outside of their direct control, they are still left with the possibility of indemnification from other controllers. Such an outcome therefore seems fair and justifiable, considering the purpose of such platforms explicitly lies in ensuring a high level of protection for individuals.

As a last step, the necessity of introducing a new, comprehensive regulation for Personal Information Management Systems, in order to ensure a more uniform regime of protection, could be considered. This notion is, however, strongly rejected here for two reasons.

First, as has been evidenced in Chapter 6: Liability outside of the GDPR of this chapter, the new strategies of the European Union, such as the Digital Strategy,[77] the Data Strategy[78] and the AI Strategy[79] have led to the enactment of an impressive amount of legislation in the last years. Furthermore, the Product Liability Directive has been updated and an update of the ePrivacy Directive might still follow. Most of these legal Acts will have some sort of impact on Personal Information Management Systems. At the same time, it must be said, that although almost a decade has by now passed since the European Data Protection Supervisor issued his Opinion 9/2016 on Personal Information Management Systems,[80] not much progress has been made since then. In spite of significant technical developments, the amount of tools and functionalities available on the market has barely evolved and still no actual holistic platform, allowing comprehensive, cross-sectional data management exists. While there are likely many reasons for the lack of progress in this area, legal uncertainties for platform providers will at least be one of those. In that sense, adding new types of regulation would only add to an arguably already over-regulated market. Furthermore, taking into account that most offerings are still in the early stages of development, it is more than likely that different risks or problems, which are currently unforeseen might arise in the future. It therefore seems far

---

[77] *European Commission,* 'Shaping Europe's digital future', https://digital-strategy.ec.europa.eu/en (accessed: 24 October 2024).

[78] *European Commission*, 'European data strategy', https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (accessed: 24 October 2024).

[79] *European Commission*, 'European approach to artificial intelligence', https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed: 24 October 2024).

[80] *EDPS*, Opinion 9/2016.

more sensible to give the businesses some time to breathe and develop properly first.

Secondly, if the suggestions included in Section C. Alternative Solutions in the GDPR were to be applied, there would be no inherent risks for the data subject at the moment. Risk for the rights and freedoms of natural persons would only arise if the overly fragmented form of interpretation on a "case-by-case" basis, applied in Part 2 Chapter 4: Designation of Roles in Personal Information Management Systems was to be followed. As has, however, been evidenced in the previous Chapter 7: Alternatives in the GDPR, there are a number of alternative interpretations which lead to a quite comprehensive and uniform regime of responsibility for Personal Information Management Systems. As long as these suggestions are followed, there seems to be no immediate need to act at the moment. Once it has been established that the PIMS will need to be considered a data controller for all processing activities related to the platform, the data subject is left with a fair and transparent counterparty with which to issue all claims against. As a result, platforms should for now be able to develop freely under the current regime, without the need for new regulation.

E. Conclusions for Part 3

Part 1 of this thesis served as an introduction into the realm of Personal Information Management Systems. Part 2 provided a legal analysis of the roles taken by those platforms under the GDPR and identified that the current regime and the form of interpreting the law lead to unsatisfactory results. This final Part 3 attempts to find alternative solutions, both within and outside of traditional data protection law.

First, the possibility of limiting the currently extremely broad scope of services offerings covered by the term Personal Information Management Systems was considered. Introducing a more limited terminology is likely to lead to a more coherent outcome when it comes to the roles taken by providers. One form of specification could relate to the technical set-up, for example, by defining specific storage types, establishing the minimal extent of covered service offering, or

the type of preferences which could be managed through the platform. Specifications might also be introduced on a personal level, governing the relationship between the parties, for example, by defining the form in which platforms may be financed or whether PIMS are intended to act in an objective or subjective manner. In the opinion presented in this thesis, the addition of three requirements would be most beneficial. Firstly, the platform should act in a neutral manner, Secondly, it should be independent from other actors. And thirdly, it should allow data management throughout the entire data lifecycle. While introducing a binding definition would likely require the enactment of a new law, there may be less intrusive measures to steer the development of the market. EU bodies such as the European Data Protection Supervisor, the European Commission, the European Data Protection Board, or the Supervisory Authorities could, for example, introduce new guidelines, further specifying the terminology. Similarly, the establishment of codes of conduct or certifications for PIMS might lead to more standardisation in the area.

Alternative forms of deriving liability and responsibility for Personal Information Management Systems outside of the GDPR have been discussed as a second step. Most types of PIMS will fall within the term data intermediation services under the Data Governance Act. Consequently, they will be subject to the conditions and notification procedures established therein. They are also likely to be considered as data holders and data processing services under the Data Act, meaning that they might receive requests for data access and will also need to ensure interoperability with other services. Also relevant in that regard is the Digital Services Act, which introduces the term of intermediary services, applicable to PIMS. Connected to that role are extensive transparency obligations, as well as the requirement to designate points of contact for both service recipients and authorities. Intermediary services under the DSA furthermore need to introduce mechanisms for the submission of notifications concerning illegal content. While not having much impact at the moment, the AI Act has also been established as quite relevant for the future of PIMS, assuming that the rise of AI will also affect them. While PIMS using AI technology are still unlikely to fall within the categories of prohibited or high-risk systems, they will have to comply with the AI Act's

transparency requirements. Furthermore, the presumption of causality introduced by the AI Liability Directive might also apply to Personal Information Management Systems in that context. This will, however, depend on whether the tool will in fact be considered a controller or processor under the GDPR. Finally, while it is not clear whether PIMS could be considered as products under the current Product Liability Directive, they are certainly covered by the new Privacy Liability Directive, adopted on October 10, 2024, which also introduces a requirement to provide upgrades, as long as the provider exercises control over the system.

While these laws introduce both additional responsibilities and forms of liability, none of them truly cover all Personal Information Management Systems in a comprehensive and coherent manner. Because of that fact, alternative forms of interpreting the GDPR in order to assume uniform controllership have been suggested. Based on the view presented in this thesis, factual influence can be derived from the existing relationship of trust between the parties, as well as the impression given towards the individual users, which implies a high level of care on the side of the PIMS provider. Whenever there is a lack of decision-making power on the side of the PIMS, this element will be transferred onto the tool from the data subject itself. Furthermore, PIMS can be assumed as exerting decisive influence over the processing activities in the form of enabling data transfer to and from other controllers.

As a final step, the expansion of the stage-based-approach in line with the *effet utile* of the GDPR has been suggested. Since the term processing covers singular activities, as well as several connected steps, the Regulation clearly allows for both the fragmentation and the unification of various processing activities conducted for the same purpose. Based on that, a rule of unification should be introduced where a chain of activities serves one overall purpose and appears as one consolidated action to the data subject. As a result, the service offerings of a Personal Information Management Systems should be analysed together rather than separately, leading to the uniform assignment of controllership for the whole platform. This solution ensures the effective and complete protection of the data subject as it leads to a comprehensive and coherent form of liability

of platform providers and should be considered the most fair and reasonable outcome.

Chapter 8

Final Conclusions

This thesis examined the roles taken by Personal Information Management Systems under the GDPR. The current state of service offerings has been presented and existing, as well as potential, types of services have been analysed to this effect. The result of this analysis has been deemed unsatisfactory, which is why alternative forms of defining and deriving liability were considered. The final conclusions and proposed solutions are presented here.

A. Key Findings

Each Part of this thesis contains conclusions at the end of the applicable section. These provide a more detailed overview of the most relevant findings and theories. Here, the key hypothesis established in each section will be summarised in order to provide a clear and coherent picture.

Part 1:

1. At the moment, there is no consensus in the market or within the legal literature as to what role under the GDPR might be taken by a provider of a Personal Information Management System. Considering the significant practical consequences for the individual users, this question should be explored and resolved.

2. The currently most commonly accepted definition of PIMS, introduced by the EDPS describing them as *"technologies and ecosystems, which aim to empower individuals to control the collection and sharing of their personal data"* is inherently broad and covers an extremely wide range of services.
3. In the current market, storage, transparency enhancing and consent management functionalities are the most common. Still, the existing tools are not yet at a stage of development that would truly allow an individual to manage the entirety or even a significant part of their dataflows through them. Also, considering the technical developments in other areas, surprisingly little progress has been made in the fields of PIMS since the initial idea of their creation came around.
4. The support of the individual in exercising their data subject rights under Chapter III of the GDPR is largely overlooked by PIMS providers. The only functionalities found in multiple tools relate to the right to data portability. Tools supporting access, erasure or objection are, however, scarce; no examples for supporting the restriction or rectification of data could be found. The reasons for this lack of focus of providers on supporting individuals in enforcing these rights are not clear, especially since already existing technical solutions could easily be applied.

Part 2:

5. The main roles under the GDPR which might be taken by parties are those of the data controller, the processor, joint controller, third party, or recipient. The designation of these roles must be conducted based on the actual influence and activities of the parties on the processing of personal data. It cannot be changed purely through contractual designation, where this would contradict the factual circumstances. Based on CJEU case law, the concept of controller is to be interpreted broadly in order to ensure a high level of protection of individuals. The CJEU has also established that parties

may take different roles in the context of different stages of an overall processing activity.

6. Personal Information Management Systems reviewed under Part 1 can essentially take any of the roles defined within the GDPR if the currently accepted rules of classification are applied. The outcome will depend on the specifics of the service offering, the technical specifications, the relationship with the data subject, and that with other involved entities. For example, when tasked with the identification of the individual, in the context of data subject request, or in the context of ensuring the secure transmission of datasets, for the purpose of exercising the right to restriction of processing, they will qualify as a processor. This is because the PIMS is taking over a task, legally assigned to another controller. When, however, storing personal data for the data subject, in the context of secure storage functionalities, they will act as a sole controller, as means and purposes are both determined by the PIMS. The role of a joint controller might also be taken, when ensuring the rectification of datasets through a predefined link with another controller, since here there will be an element of joint decision-making regarding the processing activity. Furthermore, the role of a third party will apply in instances where a transparency-enhancing translation of another controller's privacy policy is being provided to the data subject, as this activity does not technically involve the processing of personal data.

7. Different legal designations for services potentially seeming identical to the individual user are possible based on varying technical and contractual set-ups, as well as the relationships with other parties. For example, where the PIMS is providing direct rectification of data at the source or has created a link between datasets, they will be qualified as a joint controller. Where, on the other hand, the assurance of rectification is

facilitated through push and pull notices, they will only be considered a processor. Furthermore, a PIMS might take different roles with regards to separate functionalities offered within one platform. As a result, the extent of the PIMS responsibilities and liability might also vary significantly between providers and different service elements.

8. This result cannot be accepted from a data protection standpoint. It is severely lacking in transparency and fails to ensure the main goal of the GDPR, which is the complete and effective protection of the data subject.

Part 3:

9. Considering how broad the current definition of PIMS is, it comes as no surprise that the roles taken by the parties under the GDPR may vary. A limitation of the term may therefore result in more consistent legal designations. The current definition should be amended to include a requirement of neutrality and independence. Furthermore, the term should be reserved for holistic platforms, allowing data management throughout the entire data lifecycle. The new definition suggested in this Thesis is: *"Personal Information Management Systems are technologies and ecosystems which operate in an independent and neutral manner and which support individuals in the control, the collection and the sharing of their personal data, throughout the data lifecycle".* As a result, the three elements which have led to the most significant shifts in the roles and responsibilities taken by the PIMS would be pre-determined.

10. Legal responsibilities and liability for PIMS might also be derived from other Acts of EU Law. They are, for example, likely to be considered data intermediation services under the Data Governance Act, as well as data holders and data processing services under the Data Act, making them subject

to the conditions and procedures enshrined in those. PIMS will also be considered an intermediary service under the Digital Services Act, leading to enhanced transparency requirements and the obligation to introduce mechanisms for the submission of notifications concerning illegal content. While PIMS are unlikely to be considered as products under the current Product Liability Directive, they will certainly fall within the scope of the new Product Liability Directive adopted on October 10, 2024. Individuals would therefore have the opportunity to claim damages under the new Directive, particularly where the PIMS is not considered a data controller or processor. Furthermore, the new PLD introduces a requirement to provide upgrades as long as the provider exercises control over the system.

11. While AI technologies have not yet had a significant effect on PIMS, this is likely to occur in the future. In that sense, the AI Act and the AI Liability Directive would also have a direct impact. Although PIMS will not fall within the categories of prohibited or high-risk systems, they will need to comply with the AI Act's transparency requirements of Art. 50(1) AIA since they are intended to interact with natural persons. Also, where a duty of care can be established, PIMS will be subject to the presumption of causality introduced by the AI Liability Directive.

12. While responsibilities and liability for PIMS might also be derived from other Acts of EU Law, none of those provide a truly comprehensive and coherent framework for PIMS. Based on that, alternative forms of interpretation of the GDPR, in order to assume controllership for the PIMS, have been suggested. It is the view presented here that factual influence can be derived from the existing relationship of trust between the parties. Furthermore, the form in which these tools are presented to users creates a reasonable expectation of the side of the user for a high level of care. In instances where the PIMS lacks actual decision-making power, this element,

necessary for the assumption of controllership, will be derived from the data subject itself. Additionally, controllership can also be presumed based on the understanding that PIMS are exercising decisive influence over the processing activities by constituting the main element enabling data transfers in the first place.

13. The stage-based-approach introduced by the CJEU should be expanded in consideration of the *effet utile* of the GDPR. The term "processing" in the meaning of the Regulation allows for both the separation into singular steps and activities, as well as the bundling into one. In that sense, both the fragmentation and the unification of various processing activities conducted for the same purpose is possible. Fragmentation should, therefore, occur where this serves the purpose of ensuring effective and complete protection of the data subject. Where, on the other hand, fragmentation leads to the opposite result, a new approach of unification should be taken. Here the chain of activities serving one overall purpose and appearing as one consolidated action to the data subject should be considered as one processing activity, for which only one role can be taken. This approach will lead to the uniform assignment of controllership for all Personal Information Management Systems. In turn, the right and freedoms of the individual will be fully protected and a comprehensive and coherent form of liability of platform providers ensured.

B. Outlook on the Future

The concept of Personal Information Management Systems remains intriguing. While not as trendy as at the beginning of its conception, there are still several relevant developments in the field. Unfortunately, PIMS have not yet managed to fully reach their potential or fulfil the promises of ultimate user empowerment initially proclaimed. As has been concluded in Part 1, the current state of service offerings is surprisingly limited. Also, little progress has been made

since the idea of creating such platforms originally was devised. It seems that after a period of intense fascination, the field has stagnated for some time.

This stagnation is, however, likely to shift soon and PIMS might be on the verge of a new golden era. Firstly, EU lawmakers have again attempted to strengthen this notion by introducing data intermediation services and intermediary services in the Data Governance Act and the Digital Services Act respectively. In that sense intermediary platforms, are now given a clear mandate and are subject to less legal uncertainly. The same tendency can also be observed in national regulation, such as the German TDDDG, where § 26 introduced the notion of recognised consent management platforms. Also, the rapid development of AI technology may result in significant progress for PIMS. Not only transparency enhancing technologies can benefit from natural language processing. The entire field of data subject requests has the potential for full or at least partial automation, taking away much of the administrative burden from the individual. In that sense, the notion of privacy enhancing technologies is now more relevant than ever, with a vast array of potential.

Once progress has been made and Personal Information Management Systems have reached a more mature state in actually allowing the management of significant dataflows, a review of the findings contained herein might be necessary. Also, accounted for in the future might be shifts within social structures and perspectives. The rise of the internet and social media have brought significant changes in that regard and the same is likely to apply as a result of the new developments made in AI technology. How data privacy is viewed by data subjects, what elements will be considered relevant, and what type of new risks could arise, might all change within a foreseeable timeframe. The need for an interdisciplinary approach including both social and behavioural aspects, as well as technological knowledge into the legal analysis, will therefore continue to rise in significance. In that sense, this field of research will need to remain dynamic, adjusting to the current state of technological as well as societal developments.

Literaturverzeichnis

Abiteboul, Serge / Stoyanovich, Julia, 'Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation', 11 JDIQ 2019. 1 - 9.

Acquisti, Alessandro, 'Privacy in Electronic Commerce and the Economics of Immediate Gratification', in: Breese, Jack/Feigenbaum, Joan/Seltzer, Margo (eds), EC '04: Proceedings of the 5th ACM Conference on Electronic Commerce, New York 2004, 21-29.

- —/*Grossklags, Jens*, 'Losses, Gains, and Hyperbolic Discounting: Privacy Attitudes and Privacy Behavior', in: Camp, Jean L./Lewis. Stephen (eds), Economics of Information Security, 1st edn, New York 2004, 165-178.
- —/*Grossklags, Jens*, 'Privacy and rationality in individual decision making', 3 IEEE Security & Privacy 2005, 26-33.
- —/*Gross, Ralph*, 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook' in Danezis, George/Golle, Philippe (eds), Privacy Enhancing Technologies, Berlin, Heidelberg 2006, 36-58.
- —/*Grossklags, Jens*, 'What Can Behavioral Economics Teach Us about Privacy?, in: Gritzalis, Stefanos/Lambrinoudakis, Costos/Di Vimercati, Sabrina (eds), Digital Privacy Theory, Technologies, and Practices, 1st edn, New York, London 2008.
- —/*John, Leslie K./Loewenstein, George*, 'The Impact of Relative Standards on the Propensity to Disclose', 49 J. Mark. Res. 2012, 160-174.
- — /*John, Leslie K./Loewenstein, George*, 'What Is Privacy Worth?', 42 J. Leg. Stud. 2013, 249-274.
- —/*Brandimarte, Laura/Loewenstein, George*, 'Privacy and human behavior in the age of information', 347 Science 2015, 509-514.
- —/*Adjerid, Idris/Balebako, Rebecca/Brandimarte, Laura/Cranor, Lorrie Faith/Komanduri, Saranga/Leon, Pedro Giovanni/Sadeh, Norman/Schaub, Florian/Sleeper, Manya/Wang, Yang/Wilson, Shomir*, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online', 50 ACM Comput. Surv. 2017, 1-41.
- —/*Fong, Christina*, 'An Experiment in Hiring Discrimination via Online Social Networks', 66 Manag. Sci. 2020, 1005-1024.

Adjerid, Idris/Acquisti, Alessandro/Brandimarte, Laura/Loewenstein, George, 'Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency', in:

Bauer, Lujo/Beznosov, Konstantin (eds), SOUPS '13: Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle 2013, 1-11.

Adler, Mark, 'The Plain Language Movement' in Solan, Lawrence M./Tiersma, Peter M. (eds), The Oxford Handbook of Language and Law, 1st edn, Oxford 2012, 67-83.

Ahlden, Andreas, 'Braucht Jede Marke Eine Facebook-Fanpage?', in: Schulten, Matthias/Mertens, Artur/Horx, Andreas (eds), Social Branding, Wiesbaden 2012, 43-64.

Al Nasar, Mohammad Ruston/Mohd, Masnizah/Mohamad Ali, Nazlena, 'Personal Information Management Systems and Interfaces: An Overview', in: Noah, Shahrul Azman Mohd/Omar, Nazlia/Crestani, Fabio/Mohd, Masnizah/Abdul Aziz, Mohd Juzaiddin/Puade, Onn Azraai (eds), 2011 International Conference on Semantic Technology and Information Retrieval (IEEE 2011), 197-202.

Al-Ali, Rima/Hnetynka, Petr/Havlik, Jiri/Krivka, Vlastimil/Heinrich, Robert/Seifermann, Stephan/Walter, Maximilian/Juan-Verdejo, Adrian, 'Dynamic Security Rules for Legacy Systems', in: Duchien, Laurence/Trubiani, Catia/Scandariato, Riccardo/Mirandola, Raffaela/Navarro Martinez, Elena Maria/Weyns, Danny/Koziolek, Anne/Scandurra, Patrizia/Quinton, Clément (eds), ECSA '19: Proceedings of the 13th European Conference on Software Architecture, Paris 2019, 277-284.

Albalwy, Faisal/Brass, Andrew/Davies, Angela, 'A Blockchain-Based Dynamic Consent Architecture to Support Clinical Genomic Data Sharing (ConsentChain): Proof-of-Concept Study', 9 JMIR 2021, e27816.

Albanese, Guiseppe/Calbimonte Jean-Paul/Schumacher, Michael/Calvaresi, Davide, 'Dynamic Consent Management for Clinical Trials via Private Blockchain Technology', 11 J Ambient Intell Human Comput 2020, 4909-4926.

Albrecht, Jan Philipp, 'Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung', 2 CR 2016, 88-98.

Alheit K, 'The applicability of the EU product liability directive to software', 34 CILSA 2001, 188-209.

ALLEA, 'The European Code of Conduct for Research Integrity', Berlin 2017.

Alpers, Sascha/Betz, Stefanie/Fritsch, Andreas/Oberweis, Andreas/Schiefer, Gunther/Wagner, Manuela, 'Citizen Empowerment by a Technical Approach for Privacy Enforcement', in: Méndez Muñoz, Víctor/Ferguson, Donald/Helfert, Markus/Pahl, Claus (eds), Proceedings of the 8th International Conference on

Cloud Computing and Services Science (CLOSER 2018), Madeira 2018, 589-595.

— —/*Erdogan, Enes/Gapp, Stefan/Fritsch, Andreas/Miller-Askar, Ainara/Oberweis, Andreas/Schiefer, Gunther/Wagner, Manuela*, 'PRIVACY – AVARE: Selbstdatenschutz für Bürger mithilfe von Open-Source-Software', in: Klewitz-Hommelsen, Sayeed/Lang, Martin/Schönbach, Bernd (eds), Proceedings of the 13th Free and Open Source Conference (FrOSCon 2018), Bonn-Rhein-Sieg 2021, 2-12.

Alves e Silva, Marlene Sofia/da Silva Lima, Carlos Guilherme, 'The Role of Information Systems in Human Resource Management', in: Pomffyova, Maria (ed), Management of Information Systems (IntechOpen 2018).

Ambrock, Jens, 'Mitarbeiterexzess im Datenschutzrecht - Verantwortlichkeit und Haftung für Verstöße gegen die DS-GVO durch Beschäftigte', 10 ZD 2020, 492-497.

Ambrose, Karen, 'Scientific Research Data Management Policy', https://www.crick.ac.uk/sites/default/files/2018-07/crick_scientific_research_data_management_policy_0.pdf> 18 January 2016, accessed: 26 February 2026.

Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio, 'Leitlinien zum Datenschutz in den Telemedien- und Social-Media-Angeboten der Rundfunkanstalten', September 2016.

Ariely, Dan/Loewenstein, George/Prelec, Drazen, '"Coherent Arbitrariness": Stable Demand Curves Without Stable Preferences', 118 QJE 2003, 73-105.

Armbrust, Michael/Fox, Armando/Griffith, Rean/Joseph, Anthony D./Katz, Randy/Konwinski, Andy/Lee, Gunho/Patterson, David/Rabkin, Ariel/Stoica, Ion/Zaharia, Matei, 'A View of Cloud Computing', 53 Commun. ACM 2010, 50-58.

Arning, Marian/Moos, Flemming/Schefzig, Jens, 'Vergiss(,) Europa! Ein Kommentar zu EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 – Google/Mario Costeja Gonzalez', 30 CR 2014, 447-456.

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007.

— —, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010.
— —, Opinion 3/2010 on the principle of accountability, 13 July 2010.
— —, Opinion 15/2011 on the definition of consent, 13 July 2011.
— —, Opinion 04/2012 on Cookie Consent Exemption, 7 June 2012.

— —, Working Document 02/2013 providing guidance on obtaining consent for cookies, 2 October 2013.
— —, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014.
— —, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.
— —, Guidelines on Data Protection Officers ('DPOs'), 5 April 2017.
— —, Guidelines on the right to data portability, 05 April 2017.
— —, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October 2017.
— —, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018.
— —, Guidelines on Personal data breach notification under Regulation 2016/679, 6 February 2018.
— —, Guidelines on consent under Regulation 2016/679, 10 April 2018.
— —, Guidelines on transparency under Regulation 2016/679, 11 April 2018.

Assion, Simon (ed), TTDSG, 1st edn, Baden-Baden 2022.
— *—/Willecke, Lukas*, 'Der EU Data Act - Die neuen Regelungen zu vernetzten Produkten und Diensten', 11 MMR 2023, 805-810.

Association of Universities in the Netherlands, 'The Netherlands Code of Conduct for Academic Practice - Principles of good academic teaching and research' The Hague 2014.

Attoresi, Massimo/Moraes, Thiago, 'TechDispatch #3/2020 - Personal Information Management Systems', European Union 2021.

Auer-Reinsdorff, Astrid/Conrad, Isabell, Handbuch IT- und Datenschutzrecht, 3rd edn, München 2019.

Ausloos, Jef, 'The 'Right to be Forgotten' – Worth remembering?', 28 CLSR 2012, 143-152.
— *—/Dewitte, Pierre*, 'Shattering one-way mirrors – data subject access rights in practice', 8 IDPL 2018, 4-28.

Austin, Lisa, 'Privacy and the Question of Technology', 22 Law and Philosophy 2003, 119-166.
— *—/Lie, David/Sun, Peter Yi Ping/Spillette, Robin/D'Angelo, Mariana/Wong, Michelle*, 'Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project', IT3 LAB, June 2018.

Backes, Julian/Backes, Michael/Dürmuth, Marlus/Gerling, Sebastian/Lorenz, Stefan, 'X-pire! - A digital expiration date for images in social networks', arXiv preprint arXiv:1112.2649, 12 Dec 2011.

Backes, Michael/Gerling, Sebastian/Lorenz, Stefan/Lukas, Stephan, 'X-pire 2.0: a user-controlled expiration date and copy protection mechanism', in: Cho, Yookun/Shin, Sung Y. (eds.), SAC '14: Proceedings of the 29th Annual ACM Symposium on Applied Computing, New York 2014, 1633-1640.

Baek, Young Min, 'Solving the Privacy Paradox: A Counter-Argument Experimental Approach', 38 CHB 2014, 33-42.

Balkin, Jack M., 'The Fiduciary Model of Privacy', 133 HARV. L. REV F. [2020], 11-33.

Banasiński, Cezary/Rojszczak, Marcin, 'Cybersecurity of consumer products against the background of the EU model of cyberspace protection', 7 J. Cybersecur 2021, 1-15.

Barnett, Kendra, 'Google's $400m penalty and impact of the 5 heftiest data privacy fines on 2023 ad plans', https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans, 15 November 2022, accessed: 25 February 2026.

Barredo Arrieta, Alejandro/Díaz-Rodríguez, Natalia/Del Ser, Javier/Bennetot, Adrien/Tabik, Siham/Barbado, Alberto/Garcia, Salvador/Gil-Lopez, Sergio/Molina, Daniel/Benjamins, Richard/Chatila, Raja/Herrera, Francisco, 'Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI', 58 IF 2020, 82-115.

Barth, Susanne/de Jong, Menno, 'The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review', 34 TELEMAT INFORM 2017, 1038-1058.

— *—/de Jong, Mennoo/Junger, Marianne/Hartel, Pieter H./Roppelt, Janina C.,* 'Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors Among Users with Technical Knowledge, Privacy Awareness, and Financial Resources', 41 TELEMAT INFORM 2019, 55-69.

Barton, Adrien/Grüne-Yanoff, Till, 'From Libertarian Paternalism to Nudging—and Beyond', 6 Rev. Philos. Psychol. 2015, 341-359.

Bashir, Muhammad Ahmad/Wilson, Christo, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem', PoPETs 2018, 85-103.

Bassini, Marco, 'Data Controller: A Shifting Paradigm in the Digital Age' [2019] 13 BLP 2019, 103-127.

Bauer, Mareike Fenja, 'Personal Information Management mit dem Notizverwaltungs-Tool Evernote', 1 Young Information Scientist 2016, 45-57.

Baumann, Johannes/Alexiou Eleni, 'Cookie-Walls und die Freiwilligkeit von Nutzereinwilligungen - Wie fest darf die Cookie-Wall stehen?', 7 ZD 2021, 349-353.

Baumgartner Ulrich / Hansch Guido, 'Onlinewerbung und Real-Time-Bidding - Datenschutzrechtliche Fragen im Lichte der BGH-Entscheidung Cookie-Einwilligung II', ZD 2020, 435 - 439.

Bawden, David/Holtham, Clive/Courtney, Nigel, 'Perspectives on information overload', 51 Aslib Proceedings 1999, 249-155.

— —/Robinson, Lyn, 'Information Overload: An Introduction', in: Hannah, Erin (ed), Oxford Research Encyclopedia of Politics, https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1360, 30 June 2020, accessed: 05 March 2026.

Bechtolf, Hans/Vogt, Niklas, 'Datenschutz in der Blockchain – Eine Frage der Technik - Technologische Hürden und konzeptionelle Chancen', 2 ZD 2018, 66-71.

Beck, Hanno, Behavioral Economics - Eine Einführung, 1st edn, Wiesbaden 2014.

Becker, Maximilian, 'Consent Management Platforms und Targeted Advertising Zwischen DSGVO und ePrivacy-Gesetzgebung - Real Time Bidding auf Basis von Nutzerprofilen als Ausprägung der Personendatenwirtschaft', 37 CR 2021, 87-98.

Becker, Regina/Thorogood, Adrian/Bovenberg, Jasper/Mitchell, Colin/Hall, Alison, 'Applying GDPR roles and responsibilities to scientific data sharing', 12 IDPL 2022, 207-219.

— *—/Chokoshvili, David/Comandé, Giovanni/Dove, Edward S./Hall, Alison/Mitchell, Colin/Molnár-Gábor, Fruzsina/Nicolàs, Pilar/Tervo, Sini/Thorogood, Adrian*, 'Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers?', 30 EJHL 2023, 129-157.

Bell, Victoria, 'Facebook and Google are profiting off your data, now you can too: Firm launches 'ethical' data sharing platform so users can sell their OWN information to companies for money', https://www.dailymail.co.uk/sciencetech/article-6653517/Firm-launches-ethical-data-platform-users-sell-data.html, 31 January 2019, accessed: 25 February 2026.

Bellmann, Christian, 'Datenschutz bremst globales Handeln aus', https://www.sueddeutsche.de/wirtschaft/datenschutz-schrems-ii-europaeischer-gerichtshof-eugh-allianz-gdv-hannover-rueck-1.5481309, 6 Dezember 2021, accessed: 05 March 2026.

Bennett, Steven C., 'The "Right to Be Forgotten": Reconciling EU and US Perspectives', 30 Berkeley J. Int. Law 2012, 161-195.

Berger, Maria/Eisendle, David, 'Web 2.0 and the Concept of 'Data Controller': Recent Developments in EU Data Protection Law', 15 IJLT 2019, 20-39.

Bergman, Olaf/Beyth-Marom, Ruth/Nachmias, Rafi/Gradovitch, Noa/Whittaker, Steve, 'Improved search engines and navigation preference in personal information management', 26 ACM Trans. Inf. Syst. 2008, 1-24.

Bergmann, Jan (ed), Handlexikon der Europäischen Union, 6th edn, Baden-Baden 2022.

Bergt, Matthias, 'Verhaltensregeln als Mittel zur Beseitigung der Rechtsunsicherheit in der Datenschutz-Grundverordnung', 10 CR 2016, 670-678.

— —,'Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag', 8 ZD 2015, 365, 366-369.

Bermejo Fernandez, Carlos/Chatzopoulos, Dimitris/Papadopoulos, Dimitrios/Hui, Pui, 'This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices', 5 Proc ACM Hum-Comput Interact 2021, 1-22.

BfDI, Leitfaden zur Datenverarbeitung im Personalrat, 20 June 2024.

— —, 23. Tätigkeitsbericht zum Datenschutz 2009 – 2010, 12 April 2011.

Blacklaws, Christina, 'Algorithms: transparency and accountability' [2018] 376 Phil. Trans. R. Soc. A. 2018, 1-6.

Blanchette, Jean-Francouis/Johnson, Deborah G., 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness', 18 TIS 2002, 33-45.

Blume, Peter Eric, 'The Inherent Contradictions in Data Protection Law', 2 IDPL 2012, 26-36.

— —, 'Controller and processor: is there a risk of confusion?', 3 IDPL 2013, 140-145.

Boehme-Neßler, Volker, 'Das Ende der Anonymität - Wie Big Data das Datenschutzrecht verändert', 40 DuD 2016, 419-423.

Böhm, Wolf-Tassilo/Halim, Valentino, 'Cookies zwischen ePrivacy und DS-GVO – Was gilt? - Anforderungen an die Verwendung von Cookies nach der aktuellen Rechtsprechung', 10 MMR 2020, 651-656.

Boneh, Dan/Lipton, Richard J., 'A Revocable Backup System', in: SSYM'96: Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography, San Jose 1996, 91-96.

Borges, Georg/Meents, Jan Geert (eds), Cloud Computing, 1st edn, München 2016.

Borghetti, Jean-Sébastien, 'France', in: Machnikowski, Piotr (ed), European Product Liability: An Analysis of the State of the Art in the Era of New Technologies, Cambridge 2016, 205-236.

Bozhanov, Bozhidar, GDPR – A Practical Guide for Developers, https://techblog.bozho.net/gdpr-practical-guide-developers/, 29 November 2017, accessed: 22 October 2025.

Bösch, Christoph/Erb, Benjamin/Kargl, Frank/Kopp, Henning/Pfattheicher, Stefan, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns', PoPETs 2016, 237-254.

Bostrom, Nick/Ord, Toby, 'The Reversal Test: Eliminating Status Quo Bias in Applied Ethics', 116 Ethics 2006, 656-679.

Botta, Jonas, 'Delegierte Selbstbestimmung? - PIMS als Chance und Risiko für einen effektiven Datenschutz' [2021] 12 MMR 2021, 946-951.

Brandimarte, Laura/Acquisti, Alessandro/Loewenstein, George, 'Misplaced Confidences: Privacy and the Control Paradox', 4 SPPS 2013, 340-347.

Brauneck, Jens, 'Der Digital Markets Act (DMA) – das neue, bessere digitale EU-Wettbewerbsrecht?', 1 RDi 2023, 27-35.

Bräutigam, Peter/Schmidt-Wudy, Florian, 'Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung', 1 CR 2015, 56-63.

Bräutigam, Tobias, ‘The Land of Confusion: International Data Transfers between Schrems and the GDPR’, in: Bräutigam, Tobias/Miettinen, Samuli (eds), Data Protection, Privacy and European Regulation in the Digital Age, Helsinki 2016, 143-177.

Breaux, Travis D. (ed), An Introduction to Privacy for Technology Professionals, 1st edn, Portsmouth 2020).

Breitbarth, Paul, 'A Risk-Based Approach to International Data Transfers', 7 EDPL 2021, 539-549.

Brink, Stefan, 'Der Beratungsauftrag der Datenschutzaufsichtsbehörden - Aufgabe, Befugnis oder Pflicht?', 2 ZD 2020, 59-62.

— —/*Eckhardt, Jens*, 'Wann ist ein Datum ein personenbezogenes Datum? - Anwendungsbereich des Datenschutzrechts', 5 ZD 2015, 205-212.

— —/*Joos, Daniel*, ‘Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie - Tatbestandlicher Umfang und Einschränkungen des Artikel 15 DS-GVO’, 11 ZD 2019, 483-488.

Brochot Guillaume/Brunini, Juliana/Eisma, Franco/Larnes, Rebekah/Lewis, Daniel J., Personal Data Stores, Cambridge 2015.

Brüggemann, Sebastian/Hötzel, Gerrit, 'Kapitel 4 Digitalisierung' in Kipker, Dennis-Kenji/Voskamp, Frederike (eds), Sozialdatenschutz in der Praxis, 1st edn, Baden-Baden 2021.

BSI, 'BS 10012:2017+A1:2018 - Data protection. Specification for a personal information management system', https://knowledge.bsigroup.com/products/data-protection-specification-for-a-personal-information-management-system?version=standard, 31 July 2018, accessed: 14 October 2024.

— —, IT-Grundschutz-Kompendium, Köln 2023.

Buchholtz, Gabriele, 'Das „Recht auf Vergessen” im Internet - Vorschläge für ein neues Schutzkonzept', 12 ZD 2015, 570-577.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, 1st edn, Tübingen 2006.

— —/*Schwichtenberg, Simon*, 'Gesundheitsdatenschutz unter der Datenschutz-Grundverordnung', 6 GuP 2016, 218-225.

— —/*Kühling, Jürgen*, ‘Die Einwilligung in der Datenschutzordnung 2018’, 41 DuD 2017, 544-548.

Bufalieri, Luca/La Morgia, Massimo/Mei, Alessandro/Stefa, Julinda, 'GDPR: When the Right to Access Personal Data Becomes a Threat', in: 2020 IEEE International Conference on Web Services (ICWS) (IEEE 2020), 75-83.

Bühler, Sonja, 'Conditional Consent as a Valid Legal Ground for Data Processing - A Misbelief?', 1 Freilaw 2019, 25-31.

Buiten, Miriam C., 'The Digital Services Act: From Intermediary Liability to Platform Regulation', 12 JIPITEC 2021, 361-380.

Bunn, Anna, 'The curious case of the right to be forgotten', 31 CLSR 2015, 336-350.

Busch, Christoph/Mak, Vanessa, 'Putting the Digital Services Act in Context: Bridging the Gap Between EU Consumer Law and Platform Regulation', 3 EuCML 2021, 109-115.

Buttarelli, Giovanni, 'The accountability principle in the new GDPR', https://www.edps.europa.eu/sites/default/files/publication/16-09-30_accountability_speech_en.pdf, 30 September 2016, accessed: 25 February 2025.

— —, 'The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?', 2 EDPL 2017, 155-159.

Buyya, Rajkumar/Yeo, Chee Shin/Venugopal, Srikumar/Broberg, James/Brandic, Ivona, 'Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility', 25 FGCS 2009, 599-616.

Panigutti, Cecilia/Hamon, Ronan/Hupont, Isabelle/Fernandez Llorca, David/Fano Yela, Delia/Junklewitz, Henrik/Scalzo, Salvatore/Mazzini, Gabriele/Sanchez, Ignacio/Soler Garrido, Jospher/Gomez, Emilia, 'The Role of Explainable AI in the Context of the AI Act', in: FAccT '23: The 2023 ACM Conference on Fairness, Accountability, and Transparency, New York 2023, 1139-1150.

Calo, M. Ryan, 'Against Notice Skepticism in Privacy (and Elsewhere)', 87 Notre Dame Law Rev 2013, 1027-1072.

— —, 'Digital Market Manipulation', 82 Geo Wash L Rev 2014, 995-1051.

Camerer, Colin F./Loewenstein, George, 'Behavioral Economics: Past, Present, Future', in: Camerer, Colin F./Loewenstein, George/Rabin, Matthew (eds), Advances in Behavioral Economics, Princeton 2004, 3-51.

Carovano, Gabriele/Finck, Michéle, 'Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy', 50 CLSR 2023, 105830.

Carvalho, Jorge Morais/Arga e Lima, Francisco/Farinha, Martim, 'Introduction to the Digital Services Act, Content Moderation and Consumer Protection', 3 RDTec 2021, 71-104.

Castelluccia, Claude/De Cristofaro, Emiliano/Francillon, Aurélien/Kaafar, Mohamed-Ali, 'EphPub: Toward Robust Ephemeral Publishing', in: 19th IEEE International Conference on Network Protocols, Washington 2011, 165-175.

Caton, Simon/Haas, Christian, 'Fairness in Machine Learning: A Survey', 56 ACM Comput. Surv. 2024, 1-38.

Cepic, Michael, 'Broad Consent: Die erweiterte Einwilligung in der Forschung', 10 ZD-Aktuell 2021, 05214.

Chang, Daphne/Krupka, Erin L./Adar, Eytan/Acquisti, Alessandro, 'Engineering Information Disclosure: Norm Shaping Designs', in: Kaye, Jofish/Druin, Allison (eds), Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, New York 2016, 587-597.

Chapin, John/Coleman, Grace, 'Optimistic Bias: What you Think, What you Know, or Whom you Know?, 11 N. Am. J. Psychol. 2009, 121-132.

Charlesworth, AJ, 'Data Protection, Freedom of information and Ethical Review Committees: Policies, Practicalities and Dilemmas', 15 Inf. Commun. Soc. 2011, 85-103.

Chaudhry, Amir/Crowcroft, Jon/Howard, Heidi/Madhavapeddy, Anil/Mortier, Richard/Haddadi, Hamed/McAuley, Derek, 'Personal Data: Thinking Inside the Box', in: Bertelsen, Olav W./Halskov, Kim/Bardzell, Shaowen/Bødker, Susanne/Iversen, Ole Sejer/Klokmose, Clemens N./Korsgaard, Henrik (eds), Critical Alternatives, Aarhus 2015, 1-4.

Chen, Jiahong, 'The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle', 4 EDPL 2018, 36-52.

- —/*Edwards, Lilian/Urquhart, Lachlan/McAuley, Derek*, 'Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption', 10 IDPL 2020, 279-293.
- —/*Dove, Edward S./Bhakuni, Himani*, 'Explicit Consent and Alternative Data Protection Processing Grounds for Health Research', in: Kosta,

Eleni/Leenes, Ronald/Kamara, Irene (eds), Research Handbook on EU Data Protection Law, 1st edn, Cheltenham 2022, 474-502.

Cheng, Fa-Chang/Wang, Yu Shan, 'The Do Not Track mechanism for digital footprint privacy protection in marketing applications', 19 JBEM 2018, 253-267.

CERT-EU and ENISA, Boosting your Organisation's Cyber Resilience - Joint Publication, 14 February 2022.

Cheung, Anne S.Y., 'Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd', 1 J. Media Law 2009, 191-217.

Chico, Victoria, 'The impact of the General Data Protection Regulation on health research', 128 Br. Med. Bull. 2018, 109-118.

Cho, Hichang/Lee, Jae-Shin/Chung, Siyoung, 'Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience', 26 CHB 2010, 987-995.

Choi, Hanbyul/Park, Jonghwa/Jung, Yoonhyuk, 'The role of privacy fatigue in online privacy behavior', 81 CHB 2018, 42-51.

Christl, Wolfie, 'Corporate Surveillance in Everyday Life - Corporate Surveillance in Everyday Life', Vienna 2017.

Ciancimino, Michele, 'AI-Based Decision-Making Process in Healthcare - Towards a More Consistent Processing of Personal Data', 5 EuCML 2022, 173-180.

Clark, Lindsay, 'Max Schrems hits Irish Data Protection Commissioner with corruption complaint', https://www.theregister.com/2021/11/24/max_schrems_files_corruption_complaint/, 24 November 2021, accessed: 25 February 2026.

Clifford, Damian/Graef, Inge/Valcke, Peggy, 'Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections', 20 GLJ 2019, 679-721.

CNIL, General Data Protection Regulation: Guide for Processors, September 2017.

Colcelli, Valentina, 'Joint Controller Agreement under the GDPR', 3 ECLIC 2019, 1030-1047.

Comandé, Giovanni, 'Italy', in Machnikowski, Piotr (ed), European Product Liability: An Analysis of the State of the Art in the Era of New Technologies, Cambridge 2016, 275-310.

Combs, Barbara/Slovic, Paul, 'Newspaper Coverage of Causes of Death', 56 Journalism Quarterly 1979, 837-849.

Conrad, Sebastian Conrad, 'Freelancer als Auftragsverarbeiter? - Einschätzung im Sinne der Datenschutz-Grundverordnung', 43 DuD 2019, 134-136.

Contissa, Guiseppe/Docter, Koen/Lagioia, Francesca/Lippi, Marco/Micklitz, Hans-W/Pałka, Przemyslaw/Sartor, Giovanni/Torroni, Paolo, 'CLAUDETTE Meets GDPR - Automating the Evaluation of Privacy Policies using Artificial Intelligence', Study Report Funded by the European Consumer Organisation (BEUC), Florence 2018.

— *—/Lagioia, Francesca/Lippi, Marco/Micklitz, Hans-Wolfgang/Pałka, Przemyslaw/Sartor, Giovanni/Torroni, Paolo*, 'Towards Consumer-Empowering Artificial Intelligence', in: Lang, Jerome (ed), IJCAI'18: Proceedings of the 27th International Joint Conference on Artificial Intelligence, Stockholm 2018, 5150-5157.

Cooper, Dylan A./Yalcin, Taylan/Nistor, Cristina/Macrini, Matthew/Pehlivan, Ekin, 'Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising', 40 JCM 2023, 235-247.

Cordeiro, A. B. Menezes, 'Civil Liability for Processing of Personal Data in the GDPR', 5 EDPL 2019, 492.

Crabtree, Andy/Lodge, Tom/Colley, James/Greenhalgh, Chris/Glover, Kevin/Haddadi, Hamed/Amar, Yousef/Mortier, Richard/Li, Qi/Moore, John, 'Building accountability into the Internet of Things: the IoT Databox model', 4 J Reliable Intell Environ 2018, 39-55.

Cranor, Lorrie Faith, 'Necessary but not sufficient: Standardized mechanisms for privacy notice and choice', 10 J. on Telecomm. & High Tech. L. 2017, 273-308.

— *—/Arjula, Manjula/Guduru, Praveen,* 'Use of a P3P user agent by early adopters', in: Jajodia, Sushil/Samarati, Pierangela (eds), WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society, Washington 2002, 1-10.

— —/*Langheinrich, Marc/Marchiori, Massimo/Presler-Marshall, Martin/Reagle, Joseph*, 'The Platform for Privacy Preferences 1.0 (P3P1.0) Specification', https://www.w3.org/TR/P3P/, 16 April 2002, accessed: 25 February 2024.

Crémer, Jacques/Crawford, Gregory S./Dinielli, David/Fletcher, Amelia/Heidhues, Paul/Schnitzer, Monika/Scott, Morton, Fiona M., 'Fairness and Contestability in the Digital Markets Act', 40 YALE J. ON REGUL. 2023, 973-1012.

Custers, Bart/Heijne, Anne-Sophie, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice', 46 CLSR 2022, 105727.

Da Bormida, Marina/Giannetsos Thanassis (eds.), 'Security, Privacy and GDPR Compliance for Personal Data Management' https://www.datavaults.eu/wp-content/uploads/2020/11/DataVaults-D2.1-Security-Privacy-and-GDPR-Compliance-for-Personal-Data-Management.pdf, accessed 21 November 2024.

Dahi, Alan/Corrales Compagnucci, Marcelo, 'Device manufacturers as controllers – Expanding the concept of 'controllership' in the GDPR', 47 CLSR 2022, 105762.

Dammann, Ulrich, 'Erfolge und Defizite der EU-Datenschutzgrundverordnung - Erwarteter Fortschritt, Schwächen und überraschende Innovationen', 7 ZD 2016, 307-314.

Data Protection Authority, Recommendation on data sanitisation and data medium destruction techniques, Brussels 2021.

Data Protection Commission, Guidance Note: Guidance on Anonymisation and Pseudonymisation, June 2019.

— —, Guidance Note: Cookies and other tracking technologies, April 2020.

Datenethikkommission, Gutachten der Datenethikkommission, October 2019.

Däubler, Wolfgang, Gläserne Belegschaften, 9th edn, Frankfurt Oder 2021.

Dausend, Tjorven, 'Der Auskunftsanspruch in der Unternehmenspraxis - Beispiel zur Bearbeitung von Betroffenenanfragen und Exkurs zur Reichweite des Auskunftsanspruchs', 3 ZD 2019, 103-107.

Day, Gregory/Stemler, Abbey, 'Are Dark Patterns Anticompetitive?', 72 Alabama Law Review 2020, 1-45.

De Baets, Antoon, 'A historian's view on the right to be forgotten', 30 IRLCT 2016, 57-66.

de Meeus, Charlotte, 'The Product Liability Directive at the Age of the Digital Industrial Revolution: Fit for Innovation?', 4 EuCML 2019, 149-154.

Deakins, John, 'What is Zero Party Data? Zero is the Hero!', https://web.archive.org/web/20240519110736/https://www.citizenme.com/what-is-zero-party-data-zero-is-the-hero/, 9 September 2022, accessed: 25 February 2026.

Dehmel, Susanne/Hullen Nils, 'Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? - Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher', 4 ZD 2013, 147.

Denga, Michael, 'Digitale Manipulation und Privatautonomie - Provozierte Erklärungen im Privatrecht', 3 ZfDR 2022, 229-260.

Desai, Anokhy, 'Is GPC the new 'do not track'?', https://iapp.org/news/a/is-gpc-the-new-do-not-track/, 25 October 2022, accessed: 25 February 2026.

Deuker, André, 'Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services', in: Bezzi, Michele/Duquenoy, Penny/Fischer-Hübner, Simone/Hansen, Marit/Zhang, Ge (eds), Privacy and Identity Management for Life, Berlin, Heidelberg 2009, 275-283.

Deutsche Forschungsgemeinschaft, 'Guidelines for Safeguarding Good Research Practice. Code of Conduct', Bonn 2022.

Di Martino, Mariano/Robyns, Pieter/Weyts, Winnie/Quax, Peter/Lamotte, Wim/Andries, Ken, 'Personal Information Leakage by Abusing the GDPR "Right of Access"', in: Richter Lipford, Heather (ed), Proceedings of the Fifteenth Symposium on Usable Privacy and Security (USENIX 2019), Santa Clara 2019, 371-386.

Dieterich, Thomas, 'Rechtsdurchsetzungsmöglichkeiten der DS-GVO - Einheitlicher Rechtsrahmen führt nicht zwangsläufig zu einheitlicher Rechtsanwendung', 6 ZD 2016, 260-266.

Diffie, Whitfield/Hellman, Martin E., 'New directions in cryptography', 22 IEEE Trans. Inf. Theory 1976, 644-654.

Dimitrova, Diana, 'The Rise of the Personal Data Quality Principle: Is it Legal and Does it Have an Impact on the Right to Rectification?' [2021] 12 EJLT 2021, 1-31.

Doan, Xengie/Selzer, Annika/Rossi, Arianna/Botes, Wilhelmina Maria/Lenzini, Gabriele, 'Context, Prioritization, and Unexpectedness: Factors Influencing User Attitudes About Infographic and Comic Consent', in: Laforest, Frédérique/Troncy, Raphael/Médini, Lionel/Herman, Ivan (eds), WWW '22: Companion Proceedings of the Web Conference 2022, New York 2022, 534-545.

Dorel, Dusmanescu/Bradic-Martinovic, Aleksandra, 'The Role of Information Systems Human Resource Management', in: Andrei, Jean/Cvijanović, Drago/Zubovic, Jovan (eds), The Role of Labour Markets and Human Capital in the Unstable Environment, Belgrade 2011.

Dovas, Maria-Urania, 'Joint Controllership – Möglichkeiten oder Risiken der Datennutzung? - Regelung der gemeinsamen datenschutzrechtlichen Verantwortlichkeit in der DS-GVO', 11 ZD 2016, 512.

Dregelies, Max, 'Digital Services Act - Überblick über den neuen Rechtsrahmen für das Internet', 12 MMR 2022, 1033-1038.

Drobek, Piotr, 'The Role of Codes of Conduct in the EU Data Protection Framework', 2 GIS Odyssey Journal 2022, 129-146.

Druckman, James N., 'Evaluating framing effects', 22 J. Econ. Psychol. 2001, 91-101.

DSK, Orientierungshilfe – Cloud Computing, 9 October 2014.
- —, Kurzpapier Nr. 16 - Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, 19 March 2018.
- —, Kurzpapier Nr. 6 - Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, 17 December 2018.
- —, Kurzpapier Nr. 11 - Recht auf Löschung / "Recht auf Vergessenwerden", 17 December 2018.
- —, Kurzpapier Nr. 13 - Auftragsverarbeitung, Art. 28 DS-GVO, 17 December 2018.
- —, Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, 17 April 2020.
- —, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, December 2022.
- —, Stellungnahme: Referentenentwurf des BMDV zur Rechtsverordnung nach § 26 Abs. 2 TTDSG, 11. Juli 2023.

Dumais, Susan/Cutrell, Edward/Cadiz, JJ/Jancke, Gavin/Sarin, Raman/Robbins, Daniel C., 'Stuff I've Seen: A System for Personal Information Retrieval and Re-Use', 49 SIGIR Forum 2016, 28-35.

Düwell, Franz Josef/Brink, Stefan, 'Auf dem Weg zu einem Beschäftigtendatenschutzgesetz', 17 NZA 2023, 1097-1098.

Eckhardt, Jens, 'DS-GVO: Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer', 3 CCZ 2017, 111-117.

Edelman, Gilad, '"Do Not Track" Is Back, and This Time It Might Work https://www.wired.com/story/global-privacy-control-launches-do-not-track-is-back/, WIRED, 7 October 2020, accessed: 22 October 2025.

EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*,* 12 March 2019.

- —, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, 4 June 2019.
- —, Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019.
- —, DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR, 10 Dezember 2019.
- —, Guidelines 3/2019 on processing of personal data through video devices, 29 January 2020.
- —, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020.
- —, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02 September 2020.
- —, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 February 2021.
- *—/EDPS*, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 9 June 2021.
- —, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 18 June 2021.
- —, Guidelines 02/2021 on virtual voice assistants, 7 July 2021.
- —, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 4 February 2023.
- —, Guidelines 01/2022 on data subject rights - Right of access, 28 March 2023.
- —, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, 24 May 2023.
- —, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy

Directive, 14 November 2023.

EDPS, Opinion 9/2016: EDPS Opinion on Personal Information Management Systems, 20 October 2016.

- —, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017.
- —, Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021.
- —, A Preliminary Opinion on data protection and scientific research, 6 January 2020.

Edwards, Lilian/Finck, Michéle/Veale, Michael/Zingales, Nicolo, 'Data subjects as data controllers: a Fashion(able) concept?' IPR 2019, https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400 (last accessed: 11.02.2026).

Efroni, Zohar/Metzger, Jakob/Mischau, Lena/Schirmbeck, Marie, 'Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing', 5 EDPL 2019, 352-366.

Ehmann, Eugen/Selmayr, Martin (eds), Datenschutz-Grundverordnung, 3rd edn, München 2024.

Elvy, Stacy-Ann, 'Paying for Privacy and the Personal Data Economy', 117 Columbia Law Rev. 2017, 1369-1460.

Engeler, Malte/Quiel, Philipp, 'Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht', 31 NJW 2019, 2201.

Engels, Barbara, 'Data portability among online platforms', 5 IPR 2016, 1-17.

Erbguth, Jörn/Fasching, Joachim Galileo, 'Wer ist Verantwortlicher einer Bitcoin-Transaktion? - Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain', 12 ZD 2017, 560-565.

Ernst, Stefan, 'Die Einwilligung Nach der Datenschutzgrundverordnung - Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO', 3 ZD 2017, 110.

Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (eds), DSGVO. BDSG, 8th edn, Hürth 2024.

Estrada-Jiménez, Jóse/Parra-Arnau, Javier/Rodríguez-Hoyos, Ana/Forné, Jordi, 'Online advertising: Analysis of privacy threats and protection approaches', 100 Comput. Commun. 2017, 32-51.

Etteldorf, Christina, ‘A New Wind in the Sails of the EU ePrivacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU under German Presidency’, 6 EDPL 2020, 567-573.

— —, 'Neue EDSA-Leitlinien zur Qualifizierung internationaler Datentransfers', 20 ZD-Aktuell 2021, 05552.

Ettig, Diana/Herbrich, Tilman, ‘Wird’s besser, wird’s schlimmer? – Das Online-Marketing zwei Jahre nach Wirksamwerden der DSGVO’, 11 K&R 2020, 719-726.

European Commission, Commission Staff Working Paper Impact Assessment (25 January 2012).

— —, COMMISSION STAFF WORKING PAPER Impact Assessment SEC(2012) 73 final (25 January 2012).

— —, An emerging offer of "personal information management services" - Current state of service offers and challenges (23 November 2016).

— —, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products (7 May 2018).

— —, Ethics and data protection (14 November 2018).

— —, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (19 February 2020).

— —, H2020 Programme Guidelines on FAIR Data Management in Horizon 2020 (26 July 2016).

— —, Adequacy decision for the EU-US Data Privacy Framework (10 July 2023).

European Law Institute, 'European Commission's Proposal for a Revised Product Liability Directive', Vienna 2023.

European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 1st edn, Luxembourg 2018.

Evans, David S., 'The Online Advertising Industry: Economics, Evolution, and Privacy', 23 JEP 2009, 37-60.

Fairfield, Joshua A. T., '"Do-Not-Track" as Contract', 14 Vanderbilt J. of Ent. and Tech. Law 2012, 545-602.

— —, 'Do-Not-Track as Default', 11 Nw. J. Tech. & Intell. Prop. 2013, 575-620.

Fairgrieve, Duncan, 'Product Liability in the United Kingdom', 4 EuCML 2019, 170-172.

— —/*Howells, Geraint*, 'Rethinking Product Liability: A Missing Element in the European Commission's Third Review of the European Product Liability Directive', 50 MLR 2007, 962-978.
— —/*Rajneri, Eleonora*, 'Is Software a Product under the Product Liability Directive? - Member State and Academic Perspectives', 1 IWRZ 2019, 24-28.

Faust, Sebastian/Spittka, Jan/Wybitul, Tim, 'Milliardenbußgelder nach der DS-GVO? - Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz', 3 ZD 2016, 120-125.

Federrath, Hannes/Fuchs, Karl-Peter/Herrmann, Dominik/Maier, Daniel/Scheuer, Florian/Wagner, Kai, 'Grenzen des „digitalen Radiergummis"', 35 DuD 2011, 403-407.

Fennelly, Nial, 'Legal Interpretation at the European Court of Justice', 20 Fordham Int'l L.J. 1996, 656-679.

Fielding, Roy T./Singer, David (eds.), 'Tracking Preference Expression (DNT)', https://w3c.github.io/dnt/drafts/tracking-dnt.html, 17 January 2019, accessed: 25 February 2026.

Finck, Michéle, 'Blockchains and Data Protection in the European Union', 4 EDPL 2018, 17-35.
— —, Blockchain Regulation and Governance in Europe, 1st edn, Cambridge 2019.
— —/*Pallas, Frank,* 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', 10 IDPL 2020, 11-36.
— —, 'Cobwebs of control: the two imaginations of the data controller in EU law', 11 IDPL 2021, 333-347.

Floreani, Samantha, 'Putting a price tag on privacy', https://www.salinger-privacy.com.au/2020/09/28/paying-for-privacy/, 28 September 2020, accessed: 07 March 2026.

Folkerts, Elena, 'Gemeinsame Verantwortlichkeit: Grenzen der Aufteilung datenschutzrechtlicher Verpflichtungen - Anforderungen an die Gestaltung von Vereinbarungen zwischen gemeinsam Verantwortlichen', 4 ZD 2022, 201-206.

Forensic Risk Alliance, 'The rise and rise of Data Subject Access Requests, https://www.forensicrisk.com/news-and-insights/the-rise-and-rise-of-data-subject-access-requests-dsars, 4 June 2020, accessed: 07 March 2026.

Fowler, Leah R./Gillard, Charlotte/Morain, Stephanie R., ‘Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications’, 21 Health Promotion Practice 2020, 679-683.

Fradera, Francesc, 'Conference Report on "Digital Revolution: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies. Challenges for Law in Practice"', 26 E.R.P.L. 2018, 707-712.

Franck, Lorenz, 'Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO)', 3 RDV 2016, 111-119.

Frantziou, Eleni, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos', 14 Hum. Rights Law 2014, 761-777.

Freiherr von dem Bussche, Axel/Zeiter, Andrea/Brombach, Tim, 'Die Umsetzung der Vorgaben der EU-Datenschutz-Grundverordnung durch Unternehmen', 23 DB 2016, 1359-1365.

Frosio, Giancarlo, 'The Right to Be Forgotten: Much Ado About Nothing', 15 Colo. Tech. LJ 2016, 307-336.

Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Washington 2012.

Funke, Michael/Wittmann, Jörn, ‘Cloud Computing – ein klassischer Fall der Auftragsdatenverarbeitung? - Anforderungen an die verantwortliche Stelle’, 5 ZD 2013, 221-228.

Galloway, Jeffrey Michael, A Cloud Architecture for Reducing Costs in Local Parallel and Distributed Virtualized Cloud Environments, University of Alabama 2013.

Gallwas, Hans-Ullrich, 'Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit', 44 NJW 1992, 2785-2790.

Galperti, Simone/Levkun, Aleksandr/Perego, Jacopo, ‘The Value of Data Records’, 91 REStud 2023, 1007-1038.

Gasser, Urs/Palfrey, John, 'Breaking Down Digital Barriers: How and When ICT Interoperability Drives Innovation', Berkman Center Publication Series 2007.

Geambasu, Roxana/Kohno, Yoshi/Levy, Amit/Levy, Henry M., 'Vanish: Increasing Data Privacy with Self-Destructing Data', 18th USENIX Security Symposium, Montreal 2009, 299-316.

Geissler, Dennis/Ströbel, Lukas, 'Datenschutzrechtliche Schadensersatzansprüche im Musterfeststellungsverfahren', 47 NJW 2019, 3414-3418.

Gellert, Raphael, 'Why the GDPR Risk-Based Approach is About Compliance Risk, and Why It's Not a Bad Thing', in: Schweighofer, Erich/Kummer, Franz/Sorge, Christopher (eds), Trends und Communities der Rechtsinformatik - Trends and Communities of Legal Informatics, Wien 2017, 527-532.

— *—/van Bekkum, Marvin/Zuiderveen Borgesius, Frederik*, 'The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making', http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html, 28 April 2021, accessed: 13 March 2026.

Geminn, Christian L./Francis, Leon/Herder Karl-Raban, 'Die Informationspräsentation im Datenschutzrecht – Auf der Suche nach Lösungen', 14 ZD-Aktuell 2021, 05335.

Geppert, Martin/Schütz, Raimund, Beck'scher TKG-Kommentar, 5th edn, München 2023.

Gerber, Nina/Gerber, Paul/Volkamer, Melanie, 'Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior', 77 Comput. Secur. 2018, 226-261.

Gerdemann, Simon/Spindler, Gerald, 'Das Gesetz über digitale Dienste (Digital Services Act) (Teil 1) - Grundlegende Strukturen und Regelungen für Vermittlungsdienste und Host-Provider', 1 GRUR 2023, 3-11.

Gerling, Rainer W., 'Das IT-Sicherheitsgesetz: purer Aktionismus oder doch mehr IT-Sicherheit?', 4 RDV 2015, 167-171.

Gerling, Sebastian R., Plugging in Trust and Privacy: Three Systems to Improve Widely Used Ecosystems, Saarland 2014.

Gierschmann, Sibylle, 'Was "bringt" deutschen Unternehmen die DS-GVO? - Mehr Pflichten, aber die Rechtsunsicherheit bleibt', 2 ZD 2016, 51-55.

— *—/Baumgartner, Ulrich (eds),* TTDSG, 1st edn, München 2023.

Giese, Julia/Stabauer, Martin, 'Factors That Influence Cookie Acceptance', in: Nah, Fiona Fui-Hoon/Siau, Keng (eds), HCI in Business, Government and Organizations, Cham 2022, 272-285.

Gil Gonzalez, Elena/de Hert, Paul/Papakonstantinou, Vagelis, 'The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?', in: Hallinan, Dara/Leenes, Ronald/Gutwirth, Serge/de Hert, Paul (eds), Data Protection and Privacy, Oxford 2020, 267-298.

Globocnik, Jure, 'On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID', 50 IIC 2019, 1033-1044.

Gluck, Joshua/Schaub, Florian/Friedman, Amy/Habib, Hana/Sadeh, Norman/Cranor, Lorrie Faith/Agarwal, Yuyraj, 'How short is too short? implications of length and framing on the effectiveness of privacy notices', in: Zurko, Mary Ellen/Consolvo, Sunny/Smith, Matthew (eds.), SOUPS '16: Proceedings of the 12th USENIX Conference on Usable Privacy and Security, Berkley 2016, 321-340.

Gola, Peter, 'Zwei Jahre neues Bundesdatenschutzgesetz - Zur Entwicklung des Datenschutzrechts seit 1991', 48 NJW 1993, 3109-3118.

- —/*Wronka, Georg*, Handbuch zum Arbeitnehmerdatenschutz: Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 4th edn, Frechen 2007.
- —/*Schulz, Sebastian,* 'DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern? - Überlegungen zur Einwilligungsbasierten Verarbeitung von Personenbezogenen Daten Minderjähriger', 10 ZD 2013, 475-481.
- —/*Heckmann, Drik (eds),* Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3rd edn, München 2022.

Goldhammer, Klaus/Wiegand, André, 'Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler', Berlin 2018.

Golla, Sebastian J., 'Das Opportunitätsprinzip für Die Verhängung Von Bußgeldern nach der DSGVO', 34 CR 2018, 353-357.

Golland, Alexander, 'Gemeinsame Verantwortlichkeit in mehrstufigen Verarbeitungsszenarien', 07 K&R 433-438.

- —, 'Das Kopplungsverbot in der Datenschutz-Grundverordnung - Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag', 3 MMR 2018, 130-135.
- —, 'Datenschutzrechtliche Anforderungen an internationale Datentransfers', 36 NJW 2020, 2593-2596.

Gomer, Richard/Mendes Rodrigues, Eduarda/Milic-Frayling, Natasa/Schraefel, M. C., 'Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies through Search', in: 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT) (IEEE 2013), Washington 2013, 549-556.

Gonçalves, Maria Eduarda, 'The risk-based approach under the new EU data protection regulation: a critical perspective', 23 J. Risk Res. 2020, 139-152.

Gong, Jingjing/Zhang, Yan/Yang, Zheng/Huang, Yonghua/Feng, Jun/Zhang, Weiwei, 'The framing effect in medical decision-making: a review of the literature', 18 Psychol Health Med 2013, 645-653.

González Fuster, Gloria, 'Inaccuracy as a privacy -enhancing tool', 12 Ethics Inf Technol 2010, 87-95.

Goodfellow, Ian/Bengio, Yoshua/Courville, Aaron, Deep Learning, 1st edn, Cambridge/London 2016.

Gorkič, Primož, 'Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.: More Control, More Data Protection for Website Visitors? (C-40/17 Fashion ID)', 5 EDPL 2019, 579-582.

Gossen, Heiko/Schramm, Marc, 'Das Verarbeitungsverzeichnis der DS-GVO - Ein effektives Instrument zur Umsetzung der neuen unionsrechtlichen Vorgaben', 1 ZD 2017, 7-13.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (eds), Das Recht der Europäischen Union, 82nd edn, München 2024.

Graef, Inge, 'Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union', 39 Telecommun. Policy 2015, 502-514.

Gross, Ralph/Acquisti, Alessandro, 'Information revelation and privacy in online social networks', in: Atluri, Vijay (ed), WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the Electronic, New York 2005, 71-80.

Gründel, Achim, 'Ermittlung des Löschbedarfs bei unstrukturierten Datenbeständen - Eine praxisnahe Herangehensweise für die routinemäßige Datenlöschung', 11 ZD 2019, 493-498.

Gündel, Katharina, 'Hauswarte und Handwerker – Auftragsverarbeiter im Sinne der DSGVO?', 12 ZWE 2018, 429-433.

Günther, Andreas, Produkthaftung für Informationsgüter, 1st edn., Köln 2001.

Gürtler, Paul, 'Praxisfragen der Auftragsverarbeitung - Handlungsempfehlungen zur Verwendung von Altverträgen', 2 ZD 2019, 51.

Haase, Martin Sebastian, 'Die Einwilligung im Datenschutzrecht – Einschränkung der Freiheit des Einzelnen durch die überzogene Forderung nach Freiwilligkeit', 3 InTeR 2019, 113-117.

Haberer, Anno, 'Anforderungen an Cookie-Banner - Einsatz von Tracking- oder Marketing-Cookies', 12 MMR 2020, 810.

Hacker, Philipp, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law', 55 Common Mark. Law Rev. 2018, 1143-1186.

- —/*Petkova, Bilyana*, 'Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers', 15 NJTIP 2017, 1-42.
- —, 'Mehrstufige Informationsanbieterverhältnisse zwischen Datenschutz und Störerhaftung - Gestufte Kontrolle – gemeinsame Verantwortung?', 12 MMR 2018, 779-784.
- —, 'Daten als Gegenleistung. Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht', 2 ZfPW 2019, 148-197.
- —, Datenprivatrecht, Tübingen 2020.
- —, 'A legal framework for AI training data—from first principles to the Artificial Intelligence Act', 13 Law, Innovation and Technology 2020, 257-301.
- —, AI Regulation in Europe, https://ssrn.com/abstract=3556532, 7 May 2020, accessed: 29 March 2026.
- —/*Passot, Jan-Hendrik*, 'Varieties of AI Explanations Under the Law: From the GDPR to the AIA, and Beyond' in *Holzinger, Andreas/Goebel, Randy/Fong, Ruth/Moon, Taesup/Müller, Klaus-Rober/Samek, Wojciech (eds)*, xxAI - Beyond Explainable AI, Vienna 2022, 343-373.
- —, 'The European AI liability directives – Critique of a half-hearted approach and lessons for the future', CLSR 2023, 105871.
- —/*Berz, Amelie*, 'Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick', 8 ZRP 2023, 226-229.

Hagemeier, Heike, 'Kryptografie – heute und zukünftig', 43 DuD 2019, 631-635.

Hagman, William/Andersson, David/Västfjäll, Daniel/Tinghög, Gustav, 'Public Views on Policies Involving Nudges', 6 Rev. Philos. Psychol. 2015, 439-453.

Hallinan, Dara/Zuiderveen Borgesius, Frederik, 'Opinions Can Be Incorrect (in Our Opinion)! On Data Protection Law's Accuracy Principle', 10 IDPL 2020, 1-13.

— *—/Bernier, Alexander/Cambon-Thomsen, Anne/Crawley, Francis P./Dimitrova, Diana/Medeiros, Clausia Bauzer/Nilsonne, Gustav/Parker, Simon/Pickering, Brian/Rennes, Stéphanie*, 'International transfers of personal data for health research following Schrems II: a problem in need of a solution', 29 Eur J Hum Genet 2021, 1502-1509.

Hanloser, Stefan, 'DSK-Orientierungshilfe für Anbieter von Telemedien - Datenschutzrechtliche Fragen zum Online-Tracking', 7 ZD 2019, 287-290.

— —, 'Keine gemeinsame Verantwortlichkeit für Datenspeicherung durch Facebook – Fashion ID', 10 ZD 2019, 455-460.

— —, 'Schutz der Geräteintegrität durch § 25 TTDSG - Neue Cookie-Regeln ab dem 1.12.2021', 8 ZD 2021, 399-403.

— —, 'Telekommunikation-Telemedien-Datenschutz-Gesetz', 3 ZD 2021, 121-122.

— —, 'Einwilligungsverwaltungsverordnung – Förderung durch zertifiziertes Vertrauen', 8 ZD 2023, 421-422.

Hänold, Stefanie, 'Die Zulässigkeit eines „broad consent" in der medizinischen Forschung – A Never Ending Story?', 2 ZD-Aktuell 2020, 06954.

— —, '9. Nationales Biobanken-Symposium 2020 – Neue Entwicklungen zum „Broad Consent" in der medizinischen Forschung', 1 ZD-Aktuell 2021, 05016.

Hansen, Marit, 'Marrying Transparency Tools with User-Controlled Identity Management', in: Fischer-Hübner, Simone/Duquenoy, Penny/Zuccato, Albin/Martucci, Leonardo (eds), The Future of Identity in the Information Society, New York 2008, 199-220.

Harbach, Marian/Hettig, Markus/Weber, Susanne/Smith, Matthew, 'Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions', in: Jones, Matt/Palanque, Philippe (eds), CHI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York 2014, 2647-2656.

Harkous, Hamza/Fawaz, Kassem/Lebret, Rémi/Schaub, Florian/Shin, Kang G./Aberer, Karl, 'Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning', Proceedings of the 27th USENIX Security Symposium, Baltimore 2018, 531-548.

— —, *Fawaz, Kassem/Shin Kang G./Aberer, Karl*, 'PriBots: Conversational Privacy with Chatbots', SOUPS, Denver, 2016.

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke (eds), UWG, 5th edn, München 2021.

Härting, Niko, Datenschutz-Grundverordnung, Köln 2016.

— —, 'Joint Controllership nach der DSGVO', ITRB 2018, 167-170.

Hartmann, Bernd J./McGuire, Mary-Rose/Schulte-Nölke, Hans, 'Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act) - Rechtliche Rahmenbedingungen für die Vertragsgestaltung', 2 RDi 2023, 49-59.

Hartung, Jürgen/Büttgen, Lisa, 'Die Auftragsverarbeitung nach der DS-GVO', 41 DuD 2017, 549-554.

— —/*Degginger, Marco*, 'Die Reichweite des datenschutzrechtlichen Auskunftsrechts', 46 DB 2021, 2744-2748.

Haselton, Martie G./Nettle, Daniel/Andrews, Paul W., 'The Evolution of Cognitive Bias', in: Buss, David M. (ed), The Handbook of Evolutionary Psychology, Hoboken 2005, 724-746.

Häuselmann, Andreas Nicolas, 'Profiling and the GDPR: Harmonised Confusion', https://jusletter.weblaw.ch/juslissues/2018/924/profiling-in-the-gdp_3b8e8a124f.html__ONCE&login=false, 12 February 2018, accessed: 04 March 2026.

Hedbom, Hans, 'A Survey on Transparency Tools for Enhancing Privacy', in: Matyáš, Vashek/Fischer-Hübner, Simone/Cvrček, Daniel/Švenda, Petr (eds), The Future of Identity in the Information Society (IFIP 2009), Heidelberg 2009, 67-82.

Heermann, Peter W./Schlingloff, Jochen (eds), Münchener Kommentar zum Lauterkeitsrecht, 3rd edn, München 2020.

Heinzke, Philippe, 'Data Act: Ein neuer Baustein des europäischen Datenrechts', 6 GRUR-Prax 2023, 154-156.

Heiss, Stefan, 'Artificial Intelligence Meets European Union Law: The EU Proposals of April 2021 and October 2020', 10 EuCML 2021, 252-286.

Helberger, Natali/Diakopoulos, Nicholas, 'ChatGPT and the AI Act', 12 IPR 2023, 1-6.

Heldt, Amelia P., 'EU Digital Services Act: The White Hope of Intermediary Regulation', in: Flew, Terry/Martin, Fiona R. (eds.), Digital Platform Regulation, Cham 2022, 69-84.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung, 1st edn, Tübingen 2016.

— —, 'Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data', 8 JIPITEC 2017, 9-26.

Hilts, Andrew/Parsons, Christopher, 'Access My Info: An application that helps people create legal requests for their personal information', PETS, Philadelphia 2015.

Hochheiser, Harry, 'The platform for privacy preference as a social protocol: An examination within the U.S. policy context', 2 ACM Trans. Internet Technol. 2002, 276-306.

Hoeren, Thomas, 'Verarbeitung personenbezogener Daten bei Religionsgemeinschaften – Zeugen Jehovas', 10 ZD 2018, 469-473.

— —, 'Die Zeugen Jehovas und das Datenschutzrecht', Verfassungsblog, https://verfassungsblog.de/die-zeugen-jehovas-und-das-datenschutzrecht/, 11 July 2018, accessed: 09 March 2026.

— *—/Sieber, Ulrich/Holznagel*, Bernd, Handbuch Multimedia-Recht, 62nd edn, München 2024.

Hofmann, Franz/Raue, Benjamin (eds), Digital Services Act, 1st edn, Baden-Baden 2023.

Hofmann, Johanna M./Johannes, Paul C., 'DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs - Begriffsklärung der entscheidenden Frage des sachlichen Anwendungsbereichs', 5 ZD 2017, 221-226.

Holtz, Leif-Erik/Nocun, Katharina/Hansen, Marit, 'Towards Displaying Privacy Information with Icons', in: Fischer-Hübner, Simone/Duquenoy, Penny/Hansen, Marit/Leenes, Ronald/Zhang, Ge (eds), 6th IFIP: Privacy and Identity Management for Life, Heidelberg 2010, 338-348.

— —/Zwingelberg, Harald/Hansen, Marit, 'Privacy Policy Icons', in: Camenisch, Jan/Fischer-Hübner, Simone/Rannenberg, Kai (eds), Privacy and Identity Management for Life, Heidelberg 2011, 279-285.

Hölzel, Julian, 'Anonymisierungstechniken und das Datenschutzrecht', 42 DuD 2018, 502-509.

Holznagel, Bernd/Hartmann, Sarah, 'Das „Recht auf Vergessenwerden" als Reaktion auf ein grenzenloses Internet - Entgrenzung der Kommunikation und Gegenbewegung', 4 MMR 2016, 228-232.

Hon, W. Kuan/Hörnle, Julia/Millard, Christopher, 'Data protection jurisdiction and cloud computing – when are cloud users and providers subject to EU data protection law? The cloud of unknowing', 26 Int. Rev. Law Comput. Technol. 2012, 129-164.

— —/*Millard, Christopher/Walden, Ian*, 'Who is responsible for 'personal data' in cloud computing? - The cloud of unknowing, Part 2', 2 IDPL 2012, 3-18.

Hong, Soundman/Lee, Sanghyun, 'Adaptive governance, status quo bias, and political competition: Why the sharing economy is welcome in some cities but not in others', 35 Gov. Inf. Q. 2018, 283-290.

Hoofnagle, Chris Jay, Federal Trade Commission Privacy Law and Policy, 1st edn, Cambridge 2016.

— —/*King, Jennifer*, 'What Californians Understand about Privacy Online', https://ssrn.com/abstract=1262130, 3 September 2008, accessed: 13 April 2026.

Horn, Nikolai/Riechert, Anne/Müller, Christian, 'A. Neue Wege bei der Einwilligung im Datenschutz – Technische, Rechtliche und Ökonomische Herausforderungen', Neue Wege bei der Einwilligung im Datenschutz – Technische, Rechtliche und Ökonomische Herausforderungen, Leipzig 2017.

Hornung, Gerrit, 'Der Personenbezug biometrischen Daten', 28 DuD 2004, 429-431.

— —/*Hofmann, Kai*, 'Ein »Recht auf Vergessenwerden«? Anspruch und Wirklichkeit eines neuen Datenschutzrechts', 68 JZ 2013, 163-170.

— —/*Hofmann, Kai*, 'Die Auswirkungen der europäischen Datenschutzreform auf die Markt- und Meinungsforschung', 4 ZD-Beilage 2017, 1-16.

Hunter, Tatum, 'Your browser can tell websites how to treat your data. But companies didn't have to listen — until now', https://www.washingtonpost.com/technology/2021/10/26/global-privacy-control-firefox/, 26 October 2021, accessed: 04 March 2026.

IAB Europe, Transparency & Consent Framework, https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf, 18 November 2020, accessed: 04 March 2026.

Ibáñez Colomo, Pablo, 'The Draft Digital Markets Act: A Legal and Institutional Analysis', 12 JECLAP 2021, 561-575.

ICO, Data controllers and data processors: what the difference is and what the governance implications are, http://traingrcy.law.uoa.gr/moodle/plugin-file.php/62/mod_resource/content/1/7%20data-controllers-and-data-processors-dp-guidance.pdf, 05 May 2014, accessed: 04 March 2026.

- —, Guidance on the use of cookies and other similar technologies, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf, 3 July 2019, accessed: 04 March 2026.
- —, Information Commissioner's Opinion: Data protection and privacy expectations for online advertising proposals, https://ico.org.uk/media2/tssjamaw/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf, 25 November 2021, accessed: 04 March 2025.
- —, 'Direct marketing - detailed guidance', https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/respect-peoples-preferences/, 05 December 2023, accessed: 15 October 2025.

Ikeda, Scott, '€405 Million GDPR Fine for Instagram Over Privacy Settings for Underage Users', https://www.cpomagazine.com/data-protection/e405-million-gdpr-fine-for-instagram-over-privacy-settings-for-underage-users/, 9 September 2022, accessed: 04 March 2026.

Irwin, Francis W., 'Stated Expectations as Functions of Probability and Desirability of Outcome', 21 Personality 1953, 329-335.

ISO, 'Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines', https://www.iso.org/standard/71670.html, 1st edn, August 2019, accessed: 14 October 2024.

Itani, Wassim/Kayssi, Ayman/Chehab, Ali, 'Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures', in: Yang, Bo/Zhu, William/Dai, Yuanshun/Yang, Laurence T./Ma, Jianhua (eds), DASC '09: 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Washington 2010, 711-716.

Janal, Ruth, 'Haftung und Verantwortung im Entwurf des Digital Services Acts', 2 ZEuP 2021, 227-274.

Jandt, Silke/Roßnagel, Alexander, 'Social Networks für Kinder und Jugendliche - Besteht ein ausreichender Datenschutz?', 10 MMR 2011, 637-642.

— —/*Kieselmann, Olga/Wacker, Arno*, 'Recht auf Vergessen im Internet - Diskrepanz zwischen rechtlicher Zielsetzung und technischer Realisierbarkeit?', 37 DuD 2013, 235-241.
— —/*Steidle, Roland (eds.)*, Datenschutz im Internet, Baden-Baden 2018.

Janic, Milena/Wijbenga, Jan Pieter/Veugen, Thijs, 'Transparency Enhancing Tools (TETs): An Overview', in: Bella, Giampaoplo/Lenzini, Gabriele (eds), Proceedings: Third Workshop on Socio-Technical Aspects in Security and Trust (STAST 2013), Piscataway 2013, 18-25.

Janssen, Heleen/Cobbe, Jennifer/Singh, Jatinder, 'Personal Information Management Systems: A User-Centric Privacy Utopia?', 9 IPR 2020, 1-25.
— —/*Cobbe, Jennifer/Norval, Chris/Singh, Jatiner*, 'Decentralized Data Processing: Personal Data Stores and the GDPR', 10 IDPL 2020, 356-384.

Jarovsky, Luiza, 'Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs)', 4 EDPL 2018, 447-458.

Jaspers, Andreas, 'Die EU-Datenschutz-Grundverordnung - Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens', 36 DuD 2012, 571-575.

Jensen, Meiko/Lauradoux, Cedric/Limniotis, Konstantinos, Pseudonymisation techniques and best practices, Athens/Heraklion 2019.

Jentzsch, Nicola, 'Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds', Berlin 2017.
— —/*Preibusch, Sören/Harasser, Andreas*, 'Study on monetising privacy. An economic model for pricing personal information', Heraklion 2012.

Johannes, Paul C./Richter, Philipp, 'Privilegierte Verarbeitung im BDSG-E - Regeln für Archivierung, Forschung und Statistik', 41 DuD 2017, 300-305.

Jones, Meg Leta/Lee, Jenny, 'Comparing Consent to Cookies: A Case for Protecting Non-Use' [2020] 53 Cornell Int'l L.J. 2020, 97-132.

Jotzo, Florian, Der Schutz personenbezogener Daten in der Cloud, 2nd edn, Baden-Baden 2020.

Jülicher, Tim/Röttgen, Charlotte/v. Schönfeld, Max, 'Das Recht auf Datenübertragbarkeit - Ein datenschutzrechtliches Novum', 8 ZD 2016, 358-362.

Jung, Alexander, 'Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO - Praktikable Ansätze für die Erfüllung ordnungsgemäßer Datenverarbeitung', 5 ZD 2018, 208-213.

— — /*Hansch, Guido*, 'Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen - Hinweis zur Umsetzung im Konzern- oder Unternehmensumfeld', 4 ZD 2019, 143-148.

Kafsack, Hendrik, 'Ist ein sicherer Datenfluss nach Amerika unmöglich?', https://www.faz.net/pro/digitalwirtschaft/nach-schrems-urteilen-ist-ein-sicherer-datenfluss-in-die-usa-unmoeglich-17350923.html, 21 May 2021, accessed: 04 March 2026.

Kahler, Thomas, 'How to 'provide' information (Art. 12 GDPR)? European Court of Justice requires active behavior', in: Kahler, Thomas (ed.), Turning Point in Data Protection Law, 1st edn, Baden-Baden 2020.

Kahneman, Daniel/Knetsch, Jack L./Thaler, Richard H., 'Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias', 5 JEP 1991, 193-206.

Kamara, Irene/Kosta, Eleni, 'Do Not Track initiatives: regaining the lost user control', 6 IDPL 2016, 276-290.

Kamp, Meike/Rost, Martin, 'Kritik an der Einwilligung - Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen', 37 DuD 2013, 80-84.

Kamps, Michael/Schneider, Florian, 'Transparenz als Herausforderung: Die Informations- und Meldepflichten der DSGVO aus Unternehmenssicht', 1 K&R-Beilage 2017, 24-29.

Karegar, Farzaneh/Pettersson, John Sören/Fischer-Hübner, Simone, 'The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention', 23 ACM Trans. Priv. Secur. 2020, 1-38.

Kartheuser, Ingemar/Nabulsi, Selma, 'Abgrenzungsfragen bei gemeinsam Verantwortlichen - Kritische Analyse der Voraussetzungen nach Art. 26 DS-GVO', 11 MMR 2018, 717-721.

Katz, Jonathan/Lindell, Yehuda, Introduction to Modern Cryptography, 2nd edn, Boca Raton 2015.

Kayali, Laura/Manancourt, Vincent, 'How Europe's new privacy rules survived years of negotiations, lobbying and drama', https://www.politico.eu/article/europe-

privacy-rules-survived-years-of-negotiations-lobbying/,10 February 2010, accessed: 04 March 2026.

Kaye, Jane/Whitley, Edgar A./Lund, David/Morrison, Michael/Teare, Harriet/Melham, Karen, 'Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks', 23 Eur J Hum Genet 2015, 141-146.

Keane, Jonathan, 'With Biden in the White House, EU officials are pushing hard for a new data-sharing pact with the U.S.', https://www.cnbc.com/2021/04/19/privacy-shield-eu-officials-pushing-hard-for-us-data-sharing-pact.html, 19 April 2021, accessed: 15 April 2026.

Keirsbilck, Bert, 'The interaction between consumer protection rules on unfair contract terms and unfair commercial practices: Perenicová and Perenic', 50 Common Mark. Law Rev. 2013, 247-263.

Kelley, Patrick Gage/Cesca, Lucia/Bresee, Joanna/Cranor, Lorrie Faith, 'Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach', in: Mynatt, Elizabeth (ed*)*, CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta 2010, 1573-1582.

Kieselmann, Olga, Data Revocation on the Internet, 1st edn, Kassel 2018.

- —*/Kopal, Nils/Wacker, Arno*, '"Löschen" im Internet - Ein neuer Ansatz für die technische Unterstützung des Rechts auf Löschen', 39 DuD 2015, 31-36.
- —*/Wacker, Arno*, 'Löschen im Internet – rechtlich gefordert und technisch möglich!', 42 DuD 2018, 437-441.

Kindt, Els/Fontanillo López, César Augusto/Czarnocki, Jan/Kanevskaia, Olia/Herveg, Jean, 'Legal study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research', Brussels 2021.

Kipker, Dennis-Kenji/Schaar, Peter, 'EAID: Vernetzte medizinische Forschung und Datenschutz', 15 ZD-Aktuell 2017, 04263.

- —, 'Der Elefant im Raum: Aktuelle Diskussion um den Drittlandtransfer personenbezogener Daten', 8 ZD 2021, 397-398.

Kirsch, Matthew S., 'Do Not Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising', 18 Rich. J.L. & Tech 2011, 1-50.

Knauff, Markus, 'Heuristiken ≠ Immer Gut und Logik ≠ Immer Schlecht', in: Fleischer, Bernhard/Lauterbach, Reiner/Pawlik, Kurt (eds), Rationale Entscheidungen Unter Unsicherheit, Berlin 2019, 15-22.

Knijnenburg, Bart/Cherry, David, 'Comics as a Medium for Privacy Notices', SOUPS, Denver 2016.

Kodde, Claudia, 'Die "Pflicht zu Vergessen" - "Recht auf Vergessenwerden" und Löschung in BDSG und DS-GVO', 3 ZD 2013, 115-118.

Kohn, Joachim, 'Der Schadensersatzanspruch nach Artikel 82 DS-GVO - Besondere Herausforderung für die Kommunalverwaltung', 11 ZD 2019, 498-502.

König, Mark Michael, Das Computerprogramm im Recht, 1st edn, Köln 1991.

Koops, Bert-Jaap, 'The Trouble with European Data Protection Law' [2014] 4 IDPL 2014, 250-261.

Koós, Clemens/Englisch, Bastian, 'Eine "neue" Auftragsdatenverarbeitung - Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs', 6 ZD 2014, 276-285.

Körner, Marita, 'Drei Jahre Beschäftigtendatenschutz unter der Datenschutzgrundverordnung', 16 NZA 2021, 1137-1143.

Kosta, Eleni, Consent in European Data Protection Law, 1st edn, Leiden 2013.

Kramer, Rudi/Schmidt, Nicole, 'Lohnbuchführung in der datenschutzrechtlichen Bewertung - Klarstellung durch Gesetzgeber: keine Auftragsverarbeitung durch Steuerberater', 4 ZD 2020, 194-200.

Kranenborg, Herke, 'Google and the Right to Be Forgotten (Case C-131/12, Google Spain)', 1 EDPL 2015, 70-79.

Kraul, Thorsten (ed), Das Neue Recht der Digitalen Dienste, 1st edn, Baden-Baden 2023.

Kraul, Torsten/Schmidt, Jens Peter, 'Plattformregulierung 2.0 – Digital Services Act und Digital Markets Act als Herausforderung für die Compliance-Organisation', 6 CCZ 2023, 177-190.

Kremer, Sascha, 'Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung? – Analyse der tatsächlichen Lebenssachverhalte zur Abgrenzung zwischen gemeinsamer Verantwortlichkeit und Auftragsverarbeitung', 35 CR 2019, 225-234.

Krivokapić, Đjordje/Adamović, Jelena, 'Impact of General Data Protection Regulation on Children's Rights in Digital Environment', 64 BLR 2016, 205-220.

Krohm, Niclas, ‘Abschied vom Schriftformgebot der Einwilligung - Lösungsvorschläge und Künftige Anforderungen’, 8 ZD 2016, 368-373.

— *—/Müller-Peltzer, Philipp*, ‘Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung - Das Aus für das Modell "Service gegen Daten"?’, 12 ZD 2017, 551-556.

Krügel, Tina, 'Das personenbezogene Datum nach der DS-GVO - Mehr Klarheit und Rechtssicherheit?', 10 ZD 2017, 455-460.

Kuebler-Wachendorff, Sophie/Luzsa, Robert/Kranz, Johann/Mager, Stefan/Syrmoudis, Emmanuel/Mayr, Susanne/Grossklags, Jens, 'The Right to Data Portability: conception, status quo, and future directions', 44 Informatik Spektrum 2021, 264-272.

Kühberger, Anton, 'The Influence of Framing on Risky Decisions: A Meta-analysis', 75 Organ. Behav. Hum. Decis. Process. 1998, 23-55.

Kühling, Jürgen, ‘Der datenschutzrechtliche Rahmen für Datentreuhänder - Was ist zu tun?’, 45 DuD 2021, 783-788.

— *—/Klar, Manuel*, 'Löschpflichten vs. Datenaufbewahrung - Vorschläge zur Auflösung eines Zielkonflikts bei möglichen Rechtsstreitigkeiten', 10 ZD 2014, 506-510.

— —'2. F. Gemeinsame Verantwortlichkeit und Auftragsverarbeitung (Art. 26 und 28 DS-GVO)', in: Kühling, Jürgen/Klar, Manuel/Sackmann, Florian, Datenschutzrecht, 5th edn, Heidelberg 2021.

— *—/Sauerborn, Cornelius*, ‘Die Sinnhaftigkeit des § 26 TTDSG - PIMS als Medizin gegen die „Cookie-Click-Fatigue“?’, 10 ZD 2022, 531-536.

— *—/Sauerborn, Cornelius*, ‘PIMS vs. Einwilligung vs. Browsereinstellungen - Wer hat bei Cookies das letzte Wort?’, 11 ZD 2022, 596-599.

— *—/Buchner, Benedikt (eds),* Datenschutz-Grundverordnung. BDSG, 4th edn, München 2024.

Kuhlmann, Stephanie A., 'Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online', 22 DePaul J. Art, Tech. & Intell. Prop. L. 2011, 229-286.

Kulk, Stefan/Zuiderveen Borgesius, Frederik, 'Freedom of Expression and ‘Right to Be Forgotten’ Cases in the Netherlands after Google Spain', 2 EDPL 2015, 113-124.

Kumkar, Lea Katharina/Roth-Isigkeit, David, 'A criterion-based approach to GDPR's explanation requirements for automated individual decision-making', 12 JIPITEC 2021, 289-300.

Kuner, Christopher/Bygrave, Lee A./Docksey, Christopher/Drechsler, Laura (eds), The EU General Data Protection Regulation (GDPR): A Commentary, 1st edn, Oxford 2020.

LaCasse, Alex, 'IAPP Privacy Tech Vendor Report', https://iapp.org/media/pdf/resource_center/2022TechVendorReport.pdf, October 2022, last accessed: 17 April 2026.

Lachenmann, Matthias, Datenübermittlung im Konzern, 1st edn, Oldenburg 2016.

Laibson, David, 'Golden Eggs and Hyperbolic Discounting', 112 QJE 1997, 443-478.

Langhanke Carmen/Schmidt-Kessel, Martin, 'Consumer Data as Consideration', 4 EuCML 2015, 218-223.

Larouche, Pierre/Peitz, Martin/Purtova, Nadya, 'Consumer privacy in network industries - A CERRE Policy Report', Brussels 2016.

Larsson, Stefan/Jensen-Urstad, Anders/Heintz, Frederik, 'Notified But Unaware: Third-Party Tracking Online', 8 CAL 2021, 101-120.

Laue, Philipp/Kremer, Sasha (eds), Das neue Datenschutzrecht in der betrieblichen Praxis, 2nd edn, Nomos 2019.

Lee, Byung-Kwan/Lee, Wei-Na, 'The effect of information overload on consumer choice quality in an online environment', 21 Psychol. Mark. 2004, 159-183.

Lee, Lauren/Cross, Samuel, '(Gemeinsame) Verantwortlichkeit beim Einsatz von Drittinhalten auf Websites - Wird das Rad unnötig neu erfunden?', 9 MMR 2019, 559-563.

Lee, Yang W/Pipino, Leo/Strong, Diane M./Wang, Richard Y., 'Process-Embedded Data Integrity', 15 JDM 2004, 87-103.

Leeb, Christina-Maria/Lorenz, Luisa, 'Datenschutzkonforme Dokumentenentsorgung - Dos and Don'ts im Unternehmen', 12 ZD 2018, 573-578.

Lefebvre, Armel/Bakhtiari, Baharak/Spruit, Marco, 'Exploring research data management planning challenges in practice', 62 Information Technology 2020, 29-37.

Lehtiniemi, Tuukka, ‘Personal Data Spaces: An Intervention in Surveillance Capitalism?’, 15 S&S 2017, 626-639.

Leibold, Kevin, 'Schadensersatz nach Art. 82 DS-GVO wegen fehlerhafter bzw. verspäteter Auskunft – Überblick über die aktuelle Rechtsprechung', 5 ZD-Aktuell 2022, 01092.

Lembke, Mark/Fischels, André, 'Datenschutzrechtlicher Auskunfts- und Kopieanspruch im Fokus von Rechtsprechung und Praxis', 8 NZA 2022, 513-521.

Leon, Pedro/Ur, Blase/Shay, Richard/Wang, Yang/Balebako, Rebecca/Cranor Lorrie Faith, ‘Why Johnny Can’t Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising’, in: Konstan, Joseph A. (ed), CHI '12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Austin 2012, 589-598.

Levin, Irwin P./Schneider, Sanda L./Gaeth, Gary J, 'All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects', 76 Organ. Behav. Hum. Decis. Process. 1998, 149.

Levitt, Mairi, ‘Relating to Participants: How Close Do Biobanks and Donors Really Want to Be?’, 19 Health Care Anal 2011, 220-230.

Lezzi, Lukas/Oberlin, Jutta Sonja, 'Gemeinsam Verantwortliche in der konzerninternen Datenverarbeitung - Eine praxisorientierte Darstellung möglicher Konstellationen', 9 ZD 2018, 398-404.

Liao, Song/Wilson, Christin/Cheng, Long/Hu, Hongxin/Deng, Huixing, ‘Measuring the Effectiveness of Privacy Policies for Voice Assistant Applications’, in: Yao, Daphne/Yin, Heng (eds), ACSAC '20: Proceedings of the 36th Annual Computer Security Applications Conference, New York 2020, 856-869.

Liepina, Rüta/Contissa, Giuseppe/Drazewski, Kasper/Lagioia, Francesca/Lippi, Marco/Micklitz, Hans-Wolfgang/Pałka, Przemyslaw/Sartor, Giovanni, ‘GDPR Privacy Policies in CLAUDETTE: Challenges of Omission, Context and Multilingualism’, in: Proceedings of the Third Workshop on Automated Semantic Analysis of Information (ASAIL 2019), Montreal 2019, 1.

Lievens, Eva/Verdoodt, Valerie, 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation', 34 CLSR 2018, 269-278.

Lindqvist, Jenna, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?', 26 Int. J. Law Inf. Technol. 2018, 45-63.

Lippi, Marco/Pałka, Przemyslaw/Contissa, Guiseppe/Lagioia, Francesca/Micklitz, Hans-Wolfgang/Panagis, Yannis/Sartor, Giovanni/Torroni, Paolo, 'Automated Detection of Unfair Clauses in Online Consumer Contracts', in: Casini, Giovanni/Wyner, Adam (eds), Legal Knowledge and Information Systems, Amsterdam 2017, 145-54.

Loayza, Allen, 'Personal information management systems: A new era for individual privacy?', https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy, 21 March 2019, accessed: 25 February 2026.

Lodato, Janice, 'Creating an Educational Digital Library: GROW a National Civil Engineering Education Resource Library', in: Dykstra-Erickson, Elizabeth/Tscheligi, Manfred (eds), CHI EA '04: CHI '04 Extended Abstracts on Human Factors in Computing Systems, Vienna 2004, 810-824.

Lomas, Natasha, 'Tech-publisher coalition backs new push for browser-level privacy controls', https://techcrunch.com/2020/10/07/tech-publisher-coalition-backs-new-push-for-browser-level-privacy-controls/, 7 October 2020, accessed: 25 February 2026.

— —, 'France fines Clearview AI maximum possible for GDPR breaches', https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/, 20 October 2022, accessed: 25 February 2026.

Loschelder, Michael/Danckwerts, Rolf (eds), Handbuch des Wettbewerbsrecht, 5th edn, München 2019.

Loy, Carolin/Baumgartner, Ulrich, 'Consent-Banner und Nudging - Tracking-Mechanismen: Wie viel „Anstupsen" ist erlaubt?', 8 ZD 2021, 404-408.

Lu, Zhengwu/Su, Jing, 'Clinical data management: Current status, challenges, and future directions from industry perspectives', 2 Open Access Journal of Clinical Trials 2010, 93-105.

Lubasz, Dominik/Davida, Zanda, 'Consumer Personal Data as a Payment – Implementation of Digital Content Directive in Poland and Latvia', in: Amatucci, Carlo/Rodina, Anita (eds.) New Legal Reality: Challenges and Perspectives, Riga 2022, 521-531.

Lücke, Oliver, 'Die Betriebsverfassung in Zeiten der DS-GVO - "Bermuda-Dreieck" zwischen Arbeitgeber, Betriebsräten und Datenschutzbeauftragten!?', 10 NZA 2019, 658-670.

Luguri, Jamie/Strahilevitz, Lior Jacob, ‘Shining a Light on Dark Patterns’, 43 Journal of Legal Analysis 2021, 43-109.

Lühmann, Tobias B./Schumacher, Pascal/Stegemann, Lea, 'Gegenwart und Zukunft kollektiver Rechtsdurchsetzung im Datenschutzrecht - Verfolgung von Datenschutzverstößen mittels Verbandsklagen und Abtretungsmodellen unter Berücksichtigung der EU-Verbandsklagenrichtlinie', 3 ZD 2023, 131-136.

Luzak, Joasia, 'A Broken Notion: Impact of Modern Technologies on Product Liability', 11 EJRR 2020, 630-649.

Lynn, Michael, 'The Psychology of Unavailability: Explaining Scarcity and Cost Effects on Value', 13 Basic Appl. Soc. Psychol 1992, 3-7.

Lynn, Theo, 'Dear Cloud, I Think We Have Trust Issues: Cloud Computing Contracts and Trust', in: Lynn, Theo/Mooney, John G./van der Werff, Lisa/Fox, Grace (eds), Data Privacy and Trust in Cloud Computing, Cham 2021, 21-42.

Lynskey, Orla, The Foundations of EU Data Protection Law*,* 1st edn, Oxford 2015.

Macenaite, Milda/Kosta, Eleni, 'Consent for processing children’s personal data in the EU: following in US footsteps?', 26 Inf. Commun. Technol. Law. 2017, 146-197.

Machell, Millicent, 'Rise in data requests costing businesses millions', https://www.hrmagazine.co.uk/content/news/rise-in-data-requests-costing-businesses-millions/, 02 November 2023, accessed: 25 February 2026.

Machnikowski, Piotr, 'Product Liability for Information products?: The CJEU Judgment in VI/KRONE -Verlag Gesellschaft mbH & Co KG, 10 June 2021 [C-65/20]', 30 E.R.P.L 2022, 191-200.

Madden, Mary/Rainie, Lee/Zickuhr, Kathryn/Duggan, Maeve/Smith, Aaron, 'Public Perceptions of Privacy and Security in the Post-Snowden Era', Pew Research Center 2015.

Mahieu, Réne L. P./Asghari, Hadi/van Eeten, Michel, 'Collectively exercising the right of access: individual effort, societal effect', 7 IPR 2018, 1-23.

— *—/van Hoboken, Joris/Asghari, Hadi*, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, “Effective and Complete Protection” and its Application to Data Access Rights in Europe', 10 JIPITEC 2019, 85-105.

— —/*van Hoboken, Joris*, 'Fashion-ID: Introducing a phase-oriented approach to data protection?', https://www.europeanlawblog.eu/pub/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/release/1, 30 September 2019, accessed: 25 February 2026.

Maldoff, Gabe/Tene, Omar, 'Born in the USA: The GDPR and the Case for Transatlantic Privacy Convergence', 17 Colo. Tech. L.J. 2019, 295-310.

Malgieri, Gianclaudio/Comandé, Giovanni, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation', 7 IDPL 2017, 243-265.

Mali, Prashant, 'Consent in privacy laws: Analysis of India's PDPB, ECPA of USA and GDPR of EU', 7 Int. J. Law 2021, 142-152.

Mamo, Nicholas/Martin, Gillian M./Desira, Maria/Ellul, Bridget/Ebejer, Jean-Paul, 'Dwarna: A Blockchain Solution for Dynamic Consent in Biobanking', 28 Eur J Hum Genet 2020, 609-626.

Mann, Parul/Parab, Nikita/Sankpal, Madhuri/Morde, Chaitrali, 'Personal Information System', 4 IJSER 2013, 681-683.

Mantelero, Alessandro/Vaciago, Guiseppe, 'Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector', in: Senigaglia, Roberto/Irti, Claudia/Bernes, Alessando (eds), Privacy and Data Protection in Software Services, Singapore 2022, 97-110.

Mantrov, Vadims, 'Newspaper Advice That Causes Damage Is Not Covered by the Product Liability Directive: The Court of Justice of the European Union's Clarification in Krone', 14 EJRR 2023, 416-422.

Manyika, James/Chui, Michael/Brown, Brad/Bughin, Jacques/Dobbs, Richard/Roxburgh, Charles/Hung Byers, Angela, 'Big data: The next frontier for innovation, competition, and productivity', McKinsey Global Institute 2011.

Marks, Demi, 'The Internet Doesn't Forget: Redefining Privacy Through an American Right to Be Forgotten', 23 ELR 2016, 41-64.

Márquez, Luis/Rosado, David G./Mouratidis, Haralambos/Mellado, Daniel/Fernández-Medina, Eduardo, 'A Framework for Secure Migration Processes of Legacy Systems to the Cloud', in: Persson, Anne/Stirna, Janis (eds), Advanced Information Systems Engineering Workshops, Cham 2015, 507-517.

Marshall, James A. R./Trimmer, Pete C./Houston, Alasdair I./McNamara, John M., 'On evolutionary explanations of cognitive biases', 28 TREE 2013, 469-473.

Martini, Mario/von Zimmermann, Georg, 'E-Mail und integrierte VoIP-Services: Telekommunikationsdienste i. S. des § 3 Nr. 24 TKG?', 23 CR 2007, 427-431.

Masatlioglu, Yusufcan/Ok, Efe A., 'Rational choice with status quo bias', 121 J. Econ. Theory 2005, 1-29.

Maschmann, Frank, 'Der Betriebsrat als für den Datenschutz Verantwortlicher', 18 NZA 2020, 1207-1215.

Mayer-Schönberger, Victor, Delete: The Virtue of Forgetting in the Digital Age, Princeton and Oxford 2011.

McDonald, Aleecia M./Cranor, Lorrie Faith, 'The Cost of Reading Privacy Policies', 4 J.L. & Pol'y for Info. Soc'y 2008, 543-568.

— *—/Reeder, Robert W./Kelley, Patrick Gage/Cranor, Lorrie Faith*, 'A Comparative Study of Online Privacy Policies and Formats', in: Goldberg, Ian/Atallah, Mikhail J. (eds), Privacy Enhancing Technologies, Springer 2009) 37-55.

McDonald, John D./Levine-Clark, Michael (eds), Encyclopedia of Library and Information Sciences, 4th edn, Boca Raton 2017.

Meaker, Morgan, 'Facebook Finally Puts a Price on Privacy: It's $10 a Month', https://www.wired.com/story/meta-facebook-pay-for-privacy-europe/, 1 November 2023, accessed: 16 October 2024.

Meinhold, Stefan, 'Stellung des Personalrats als Verantwortlicher nach der DS-GVO', 10 NZA 2019, 670-672.

Mell, Peter/Grance, Timothy, The NIST Definition of Cloud Computing, Gaithersburg 2011.

Meredith, Barbara, 'Data protection and freedom of information', 330 BMJ 2005, 490 - 491.

Metzger, Axel, 'Dienst Gegen Daten: Ein Synallagmatischer Vertrag', 6 AcP 2016, 817-865.

— *—/Schweitzer, Heike,* 'Shaping Markets: A Critical Evaluation of the Draft Data Act', 1 ZEuP 2023, 42-82.

Metzger. Miriam J., 'Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure', 33 Commun. Res. 2006, 155-179.

Möhle, Jan-Peter, Die datenschutzrechtliche Verantwortlichkeit des Betriebsrats, 1st edn, Berlin 2021.

Möhrke-Sobolewski Christine/Klas, Benedikt, 'Zur Gestaltung des Minderjährigendatenschutzes in Digitalen Informationsdiensten', 12 K&R 2016, 373-378.

Molnár-Gábor, Fruzsina, 'Germany: a fair balance between scientific freedom and data subjects' rights?', 137 Hum. Genet. 2018, 619-626.

Moloi, Tankiso/Marwala, Tshilidzi, Artificial Intelligence in Economics and Finance Theories, Cham 2020.

Monreal, Manfred, '"Der für die Verarbeitung Verantwortliche" – das unbekannte Wesen des deutschen Datenschutzrechts - Mögliche Konsequenzen aus einem deutschen Missverständnis', 12 ZD 2014, 611-616.

Monteleone, Shara, 'Addressing the 'Failure' of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation', 43 Syracuse J. Int'l L. & Com. 2015, 69-119.

Muirhead, Jessica/Grout, Vic, 'Effective age-gating for online alcohol sales', https://s3.eu-west-2.amazonaws.com/sr-acuk-craft/documents/Effective-age-gating-for-online-alcohol-sales-Final-Report.pdf, January-April 2020, accessed: 26 February 2026.

Müller, Anne-Kathrin, Software als "Gegenstand" der Produkthaftung, 1st edn, Baden-Baden 2019.

Müller, Klaus, 'Künftige Plattformregulierung und effektive Durchsetzung in Deutschland - Notwendigkeit und Umsetzung des Digital Services Act', MMR-Beilage 2022, 1007-1011.

Müthlein, Thomas, 'ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland', 2 RDV 2016, 74-87.

Mylly, Ulla-Maija, 'Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information', 54 IIC 2023, 1013-1043.

Naranjo, Diego, 'Forewords · e-Privacy Regulation: Good Intentions but a Lot of Work to Do', 3 EDPL 2017, 152-154.

Narayanan, Arvind/Mathur, Arunesh/Chetty, Marshini/Kshirsagar, Mihir, 'Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces', 18 Queue 2020, 67-92.

Nash, Victoria/O'Connell, Rachel/Zevenbergen, Bendert/Mishkin, Allison, 'Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry', Oxford 2013.

Nautsch, Andreas/Jasserand, Catherine/Kindt, Els/Todisco, Massimiliano/Trancoso, Isabel/Evans, Nicholas, 'The GDPR & Speech Data: Reflections of Legal and Technology Communities, First Steps towards a Common Understanding', INTERSPEECH, Graz 2019, 3595-3699.

Navarro, Emmanuel C., 'Human Resource Information Management System' 8 IJSR 2019, 1826-1830.

Nebel, Maxi, 'Alles abwählen: Mit der Einwilligungsverwaltungs-Verordnung gegen den Cookie-Banner-Dschungel', 16 ZD-Aktuell 2020, 01321.

Ni, Feng/Arnott, David/Gao, Shijia, 'The Anchoring Effect in Business Intelligence Supported Decision-Making', 28 Journal of Decision Systems 2019, 67-81.

Nickel, Christian, 'Alternativen der konzerninternen Auftragsverarbeitung - Können Konzernobergesellschaften Auftragsverarbeiter von Konzernuntergesellschaften sein?', 3 ZD 2021, 140-145.

Nink, Judith/Pohle, Jan, 'Die Bestimmbarkeit des Personenbezugs - Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze', 9 MMR 2015, 563-567.

Nokhbeh Zaeem, Razieh/German, Rachel L./Barber, K. Suzanne, 'PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining', 18 ACM Trans Internet Technol 2018, 1-18.

— *—/Anya, Safa/Issa, Alex/Nimergood, Jake/Rogers, Isabelle/Shah, Vinay/Srivastava, Ayush/Barber, K. Suzanne*, 'PrivacyCheck's Machine Learning to Digest Privacy Policies: Competitor Analysis and Usage Patterns', in: 2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2020), 291-298.

Nolte, Claus-George, 'Personal Data as Payment Method in SNS and Users' Concerning Price Sensitivity - A Survey', in: Abramowicz, Witold (eds.) Business Information Systems Workshops, Cham 2015, 273-282.

Nordberg, Ana, 'Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation', in: Slokenberga, Santa/Tzortzatou, Olga/Reichel, Jane (eds), GDPR and Biobanking, 1st edn, Cham 2021, 61-89.

Nouwens, Mida/Liccardi, Ilaria/Veale, Michael/Karger, David/Kagal, Lalana, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence', in: Bernhaupt, Regina/Mueller, Florian/Verweij, David/Andres, Josh (eds), CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu 2020, 1-13.

Novelli, Claudio/Casolari, Federico/Rotolo, Antionio/Taddeo, Mariarosaria/Floridi, Luciano, 'Taking AI risks seriously: a new assessment model for the AI Act', 39 AI & Soc 2024, 2493-2497.

noyb, 'Europäische Kommission gibt EU-US-Datentransfers 3. Runde beim EuGH', https://noyb.eu/de/european-commission-gives-eu-us-data-transfers-third-round-cjeu, 10 July 2023, accessed: 02 March 2026.

— —, 'Meta (Facebook / Instagram) to move to a "Pay for your Rights" approach', https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach, 3 October 2023, accessed: 03 March 2026.

OECD, The App Economy, 16 Dec 2013.

— —, Data-Driven Innovation - Big Data for Growth and Well-Being, 06 October 2015.

— —, Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper 2021.

O'Hara, Kieron, 'The Right to Be Forgotten: The Good, the Bad, and the Ugly', 19 IEEE Internet Comput. 2015, 73-79.

O'Donoghue, Ted/Rabin, Matthew, 'Choice and Procrastination' [2001] 116 QJE 2001, 121-160.

O'Loughlin, Kristen/Neary, Martha/Adkins, Elizabeth C./Schueller, Stephen M., 'Reviewing the data security and privacy policies of mobile apps for depression', 15 Internet Interv. 2019, 110-115.

O'Sullivan, Owen P., 'The Neural Basis of Always Looking on the Bright Side', 8 Dial Phil Ment Neuro Sci 2015, 11-15.

Paal, Boris P., 'Schadensersatzansprüche bei Datenschutzverstößen - Voraussetzungen und Probleme des Art. 82 DS-GVO', 1 MMR 2020, 14-19.

— *—/Pauly, Daniel A. (eds),* Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 3rd edn, München 2021.

— —, 'Höhe des Ersatzes immaterieller Schäden nach Art. EWG_DSGVO Artikel 82 DS-GVO', 51 NJW 2022, 3673-3679.

— — and Kritzer I, 'Geltendmachung von DS-GVO-Ansprüchen als Geschäftsmodell', 34 NJW 2022, 2433-2439.

Paar, Christof/Pelzl, Jan, Understanding Cryptography, 1st edn, Heidelberg 2010.

Pałka, Przemyslaw/Lippi, Marco, 'Chapter 5: Big Data Analytics, Online Terms of Service and Privacy Policies', in Vogl, Roland (ed), Research Handbook on Big Data Law, Cheltenham 2021, 115-134.

Pandit, Harshvardhan J., 'Proposals for Resolving Consenting Issues with Signals and User-side Dialogues', https://arxiv.org/abs/2208.05786, accessed: 25 March 2026.

Papadopoulou, Eliza/Stobart, Alex/Taylor, Nick K./Williams, Howard M., 'Enabling Data Subjects to Remain Data Owners', in: Jezic, Gordan/Howlett, Robert J./Jain, Lakhmi C. (eds), Agent and Multi-Agent Systems: Technologies and Applications, Cham2015, 239-248.

Pardo, Raúl/Le Métayer, Daniel, 'Analysis of Privacy Policies to Enhance Informed Consent (Extended Version)', Inria Rhone-Alpes 2019, 1-22.

Pauka, Mark/Kemper, Til, 'Eignung und Datenschutz im Vergaberecht', 2 NZBau 2017, 71-76.

Paun, Mara, 'On the Way to Effective and Complete Protection (?): Some Remarks on Fashion ID', 9 EuCML 2020, 35-37.

Pavur, James/Knerr, Casey, 'GDPArrrrr: Using Privacy Laws to Steal Identities', Blackhat USA 2019.

Peitz, Carlo, Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, 1st edn, Wiesbaden 2020.

*Peloquin, David/DiMaio, Michael/Bierer, Barbara/Barnes, Mar*k, 'Disruptive and avoidable: GDPR challenges to secondary research uses of data', 28 Eur. J. Hum. Genet. 2020, 697-705.

Peng, Lihong/Guo, Yi/Hu, Dehua, 'Information Framing Effect on Public's Intention to Receive the COVID-19 Vaccination in China' [2021] 9 Vaccines 2021, 995.

Perlman, Radia, 'The Ephemerizer: Making Data Disappear' [2005] 1 JISSec 2005, 51-68.

Petri, T, 'Auftragsdatenverarbeitung – heute und morgen - Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts', 7 ZD 2015, 305-309.

Petrlic, Ronald, 'Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO - Wie die Betroffenenrechte der DSGVO nicht zum Bumerang für die Betroffenen werden', 43 DuD 2019, 71-75.

Piltz, Carlo, 'Die Datenschutz-Grundverordnung. Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Datenverarbeitung', 9 K&R 2016, 557-567.

- —, 'Die Datenschutz-Grundverordnung. Teil 2: Rechte der betroffenen und korrespondierende Pflichten des Verantwortlichen', 10 K&R 2016, 629-636.
- — */Kühner, Jasmin*, 'Ausnahmevorschriften bei Cookie-Einwilligungen - Auslegung des Begriffs „unbedingt erforderlich" nach der ePrivacy-RL', 3 ZD 2021, 123-128.
- —, 'Das neue TTDSG aus Sicht der Telemedien — Anwendungsbereich, Tracking und Aufsichtsbehörden', 8 CR 2021, 555-565.

Podszun, Ruprecht (ed), *Digital Markets Act*, 1st edn, Baden-Baden 2023.

- —*/Pfeifer, Clemens*, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission', 13 GRUR 2022, 953-961.
- —, *Bongartz, Philipp/Kirk, Alexander*, 'Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie' [2022] 45 NJW 2022, 3249-3254.

Politou, Eugenia/Michota, Alexandra/Alepis, Efthimios/Pocs, Matthias/Patsakis, Constantinos, 'Backups and the right to be forgotten in the GDPR: An uneasy relationship', 34 CLSR 2018, 1247-1257.

Pollach, Irene, 'What's Wrong with Online Privacy Policies?', 50 Commun. ACM 2007, 103-108.

Porat, Ariel/Strahilevitz, Lior Jacob, 'Personalizing Default Rules and Disclosure with Big Data', 112 MLR 2014, 1417-1478.

Potacs, Michael, 'Effet utile als Auslegungsgrundsatz', 44 EuR 2001, 465-487.

Prictor, Megan/Teare, Harriet, J.A./Bell, Jessica/Taylor, Mark/Kaye, Jane, 'Consent for Data Processing Under the General Data Protection Regulation: Could 'Dynamic Consent' Be a Useful Tool for Researchers?', 3 JDPP 2019, 93-112.

Purtova, Nadezhda, 'The law of everything. Broad concept of personal data and future of EU data protection law', 10 L.I.T. 2018, 40-81.

Radtke, Tristan, Gemeinsame Verantwortlichkeit unter der DSGVO, 1st edn, Baden-Baden 2021.

Rajan, R. Arokia Paul/Shanmugapriyaa, S, 'Evolution of Cloud Storage as Cloud Computing Infrastructure Service', 1 IOSRJCE 2012, 38-45.

Raji, Behrang, 'Auskunftsanspruch in der Praxis - Ausgewählte Fragen zum Auskunftsrecht nach Art. EWG_DSGVO Artikel 15 DS-GVO', 6 ZD 2020, 279-284.

Rauda, Christian, 'Gemeinsamkeiten von US Children Online Privacy Protection Act (COPPA) und DS-GVO - Zustimmungserfordernis der Eltern zur Verarbeitung von Daten Minderjähriger', 1 MMR 2017, 15-19.

Raue, Benjamin/Heesen, Hendrik, 'Der Digital Services Act', 49 NJW 2022, 3537-3543.

Rauer, Nils/Ettig, Diana, 'Nutzung von Cookies - Rechtliche Anforderungen in Europa und Deren Umsetzungsmöglichkeiten', 1 ZD 2014, 27-32.

- — /*Ettig, Diana*, 'Rechtskonformer Einsatz von Cookies - Aktuelle Entwicklungen', 6 ZD 2015, 255-259.
- — /*Ettig, Diana*, 'Aktuelle Entwicklungen Zum Rechtskonformen Einsatz von Cookies - Die Rechtslage auf dem Prüfstand von Kommission und Gerichten', 9 ZD 2016, 423-427.
- — /*Ettig, Diana*, 'Update Cookies 2020 - Aktuelle Rechtslage und Entwicklungen', 1 ZD 2021, 18-24.

Reidenberg, Joel R./Breaux, Travis/Cranor, Lorrie Faith/French, Brian/Grannis, Amanda/Graves James/Liu, Fei/McDonald, Aleecia/Norton, Thomas/Ramanath, Rohan/Russell, N Cameron/Sadeh, Norman/Schaub, Florian, 'Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding', 30 BTLJ 2015, 39-68.

- —/*Bhatia, Jaspreet/Breaux, Travis D./Norton, Thomas B.,* 'Ambiguity in Privacy Policies and the Impact of Regulation', 45 J. Leg. Stud. 2016, 163-190.

Reus, Jurre/Bilderbeek, Nicole, 'Data portability in the EU: An obscure data subject right',https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/, 24 March 2022, accessed: 26 February 2026.

Rezaei, Jafar, 'Anchoring Bias in Eliciting Attribute Weights and Values in Multi-Attribute Decision-Making', 30 Journal of Decision Systems 2020, 72-96.

Richards, Neil/Hartzog, Woodrow, 'The Pathologies of Digital Consent', 96 WULR 2019, 1461-1503.

Richter, Heiko, 'Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine "Verordnung über europäische Daten-Governance"', 3 ZEuP 2021, 634-667.

Richter, Stephanie, 'Vereinbarkeit des Entwurfs zum Data Act und der DS-GVO - Der schmale Grat zwischen Schutz personenbezogener Daten und Datenkommerzialisierung', 3 MMR 2023, 163-186.

Richter, Tim, 'Der Arbeitnehmer als Verantwortlicher für die Einhaltung datenschutzrechtlicher Bestimmungen' [2020] 24 ArbRAktuell 2020, 613-616.

Riechert, Anne, 'B. Stellungnahme. Rechtliche Aspekte eines Einwilligungsassistenten', in: Neue Wege bei der Einwilligung im Datenschutz – Technische, Rechtliche und Ökonomische Herausforderungen, Leipzig 2017.

— *—/Richter, Frederick*, 'Was die DSGVO braucht: Kohärente Umsetzung und innovative Instrumente', Berlin 2021.

— *—/Wilmer, Thomas (eds)*, TTDSG, Berlin 2022.

Rieckhoff, Katharina, 'Kein Auftragsverarbeitungsvertrag mehr für Videokonferenz-Tools?', https://www.datenschutz-notizen.de/kein-auftragsverarbeitungsvertrag-mehr-fuer-videokonferenz-tools-0237051/, 10 August 2022, accessed: 26 February 2026.

Ritter, Jeffrey/Mayer, Anna, 'Regulating Data as Property: A New Construct for Moving Forward', 17 DLTR 2017, 220-277.

Ross, Derek G., 'Ambiguous Weighting and Nonsensical Sense: The Problems of "Balance" and "Common Sense" as Commonplace Concepts and Decision-making Heuristics in Environmental Rhetoric', 26 Soc. Epistemol. 2012, 115-144.

Rossi, Arianna/Palmirani, Monica, 'DaPIS: An Ontology-Based Data Protection Icon Set', in: Peruginelli, Ginevra/Faro, Sebastian (eds), Knowledge of the Law in the Big Data Age, Amsterdam 2019, 181-195.

— *—/Palmiran, Monica*, 'Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection', 36 Design Issues 2020, 82-96.

Roßnagel, Alexander, 'Konflikte zwischen Informationsfreiheit und Datenschutz?', 1 MMR 2007, 16-21.

— —, 'Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung', Kassel 2017.
— —, ‘Datenschutz in der Forschung - Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen’, 4 ZD 2019, 157-164.
— —, 'Datenlöschung und Anonymisierung - Verhältnis der beiden Datenschutzinstrumente nach DS-GVO', 4 ZD 2021, 188-192.

Rothkegel, Tobias/Strassemeyer, Laurenz, 'Joint Control in European Data Protection Law – How to make Sense of the CJEU’s Holy Trinity - A case study on the recent CJEU rulings (Facebook Fanpages; Jehovah’s Witnesses; Fashion ID)', 20 CRi 2019, 161-171.

Rouvroy, Antoinette/Poullet, Yves, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’, in: Gutwirth, Serge/Poullet, Yves/Hert, Paul/Terwangne, Cécile/Nouwt, Sjaak (eds), Reinventing Data Protection?, Dordrecht 2009, 45-76.

Rozin, Paul/Nemeroff, Carol, '11 - Sympathetic Magical Thinking: The Contagion and Similarity “Heuristics”', in: Gilovich, Thomas/Griffin, Dale/Kahneman, Daniel (eds), Heuristics and Biases, Cambridge 2012, 201-217.

Margaret Rouse, 'What Does Backup Mean?', https://www.techopedia.com/definition/1056/backup, 31 August 2023, accessed: 22 October 2024

Rücker, Daniel/Kugler, Tobial (eds), New European General Data Protection Regulation, 1st edn, Baden-Baden 2018.

Ruohonen, Jukka/Hjerppe, Kalle, 'The GDPR enforcement fines at glance', 106 Inf. Syst. 2022, 101876.

Ruschemeier, Hannah, ‘Privacy als Paradox? Rechtliche Implikationen verhaltenspsychologischer Erkenntnisse’, in: Friedew *Ruschemeier* ald, Michael/Roßnagel, Alexander/Heesen, Jessica/Krämer, Nicole/Lamla, Jörn (eds), Künstliche Intelligenz, Demokratie und Privatheit, Baden-Baden 2022, 211-238.
— —, 'Competition law as a powerful tool for effective enforcement of the GDPR', https://verfassungsblog.de/competition-law-as-a-powerful-tool-for-effective-enforcement-of-the-gdpr/, 07 July 2023, accessed: 26 February 2026.

Sadeh, Norman/Acquisti, Alessandro/Breaux, Travis D./Cranor, Lorrie Faith/McDonald, Aleecia M./Reidenberg, Joel R./Smith, Noah A./Liu, Fei/Russell, N. Cameron/Schaub, Florian/Wilson, Shomir, ‘The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing

to Semi-Automatically Answer Those Privacy Questions Users Care About', Carnegie Mellon 2013.

— *—/Acquisti, Alessandro/Breaux, Travis D./Cranor, Lorrie Faith/McDonald, Aleecia M./Reidenberg, Joel R./Smith, Noah, A/Liu, Fei/Russel N. Cameron/Schaub, Florian/Wilson, Shomir/Graves, James T./Leon, Pedro Giovanni/Ramanath, Rohan/Rao, Ashiwi,* 'Towards Usable Privacy Policies: Semi-automatically - Extracting Data Practices From Websites' Privacy Policies', SOUPS, Menlo Park 2014.

Sadl, Urska, 'The role of effet utile in preserving the continuity and authority of European Union law: evidence from the citation web of the pre-accession case law of the court of justice of the EU', 8 EJLS 2015, 18-45.

Saemann, Marlene/Theis, Daniel/Urban, Tobias/Degeling, Martin, 'Investigating GDPR Fines in the Light of Data Flows', in: Kerschbaum, Florian/Mazurek, Michelle L. (eds), Proceedings on Privacy Enhancing Technologies, Warsaw 2022, 314-331.

Sahin, Yagmur, 'Gdpr and Implementation Issues', Medium, https://medium.com/databulls/is-europes-data-protection-regulation-gdpr-on-the-verge-of-collapse-844a2fa7dd6, 7 June 2021, last accessed: 16 October 2024.

Samuelson, William/Zeckhauser, Richard, 'Status quo bias in decision making', 1 JF Risk Uncertainty 1988, 7-59.

Sandfuchs, Barbara, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II', 3 GRUR Int. 2021, 245-249.

Santos, Cristiana/Nouwens, Midas/Toth, Michael/Bielova, Nataliia/Roca, Vincent, 'Consent Management Platforms Under the GDPR: Processors and/or Controllers?', in: Gruschka, Nils/Antunes, Luís Filipe Coelho/Rannenberg Kai/Drogkaris, Prokopios (eds), Privacy Technologies and Policy, Cham 2021, 47-69.

Sarkar, Subhadeep/Banâtre, Jean-Pierre/Rilling, Louis/Morin, Christine, 'Towards Enforcement of the EU GDPR: Enabling Data Erasure', Things 2018 - 11th IEEE International Conference of Internet of Things, Halifax 2018, 1-8.

Sarunski, Maik, 'Big Data – Ende der Anonymität? - Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern', 40 DuD 2016, 424-427.

Sattler, Andreas, Informationelle Privatautonomie, 1st edn, Tübingen 2022.

Schaar, Katrin, ‘Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte - Die informierte Einwilligung nach der DS-GVO und den Ethikrichtlinien’, 5 ZD 2017, 213-220.

Schantz, Peter, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht', 26 NJW 2016, 1841-1847.

— — */Wolff, Heinrich Amadeus*, Das neue Datenschutzrecht, 1st edn, München 2017.

Schätzle, Daniel, ‘Ein Recht auf die Fahrzeugdaten - Das Recht auf Datenportabilität aus der DS-GVO’, 2 PinG 2016, 71-75.

— —, ‘Zum Kopplungsverbot der Datenschutz-Grundverordnung - Warum auch die DSGVO kein absolutes Kopplungsverbot kennt’, 5 PinG 2017, 203-208.

Schaub, Florian/Balebako, Rebecca/Durity, Adam L./Cranor, Lorrie Faith, 'A Design Space for Effective Privacy Notices', SOUPS 2015, Ottawa 2015.

Schermer, Bart Willem/Custers, Bart/van der Hof, Simone, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection', 16 Ethics Inf Technol 2014, 171-182.

Schlee, Nelli, 'EuGH: Fashion ID: Gemeinsame Verantwortlichkeit 3.0', 14 ZD-Aktuell 2019, 06762.

Schleipfer, Stefan, 'Pseudonymität in verschiedenen Ausprägungen - Wie gut ist die Unterstützung der DS-GVO?', 6 ZD 2020, 284-291.

Schmidt, Birgit/Kuchma, Iryna, Implementing Open Access Mandates in Europe, 1st edn, Göttingen 2012.

— —*/Babilon, Tobias,* ‘Anforderungen an den Einsatz von Cookies, Browser-Fingerprinting und Ähnlichen Techniken im Deutschen Recht’, 2 K&R 2016, 86-90.

Schmidt-Kessel, Martin/*Grimms, Anna*, ‘Unentgeltlich oder Entgeltlich? – Der Vertragliche Austausch von Digitalen Inhalten Gegen Personenbezogene Daten’, 1 ZfPW 2017, 84-108.

Schmitz, Barbara, 'Digitale-Gesetze-Strategie – Agilität oder „Act“ionismus?' [2022] 4 ZD 2022, 189.

— —, 'BMDV: Referentenentwurf zur Einwilligungsverwaltung nach § TTDSG § 26 TTDSG', 14 ZD-Aktuell 2023, 01304.

Schmon, Christoph, 'Product Liability of Emerging Digital Technologies - A Fitness Check of the 1985 Product Liability Directive', 6 IWRZ 2018, 254-259.

Schneider, Jochen/Härting, Niko, 'Wird der Datenschutz nun endlich internettauglich? - Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht', 5 ZD 2012, 199-203.

Schreiber, Kristina, 'Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden - Anwendungsbereiche, Vertragsgestaltung und Folgen nicht gleichwertiger Verantwortung', 2 ZD 2019, 55-60.

— —, 'Revolutioniert der Data Act die Datenwirtschaft?', 8 MMR 2023, 541-542.

Schrey, Joachim/Thalhofer, Thomas, 'Rechtliche Aspekte der Blockchain', 20 NJW 2017, 1431-1436.

Schröder, Christian/Haag, Nils Christian, 'Neue Anforderungen an Cloud Computing für die Praxis - Zusammenfassung und erste Bewertung der „Orientierungshilfe – Cloud Computing"', 4 ZD 2011, 147.

Schuett, Jonas, 'Risk Management in the Artificial Intelligence Act', 15 EJRR 2024, 367-386.

Schumacher, Pascal, 'TEIL 5: Datenschutz', in: Bräutigam , Peter (ed), IT-Outsourcing und Cloud-Computing, Berlin 2019, 432-517.

— —/*Sydow, Lennart/von Schönfeld, Max*, 'Cookie Compliance, Quo Vadis? - Datenschutzrechtliche Perspektiven für den Einsatz von Cookies und Webtracking nach TTDSG und ePrivacy-VO', 8 MMR 2021, 603-609.

Schumann, Heribert/Mosbacher, Andreas/König, Stefan (eds), Medienstrafrecht, 1st edn, Baden-Baden 2023.

Schwartmann, Rolf/Weiß, Steffen (eds.), 'Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017', Fokusgruppe Datenschutz des Digital-Gipfels, Ludwigshafen 2017.

— —/*Weiß, Steffen (eds.),* 'Datenmanagement- und Datentreuhandsysteme', https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=1, 30 November 2020, accessed: 12 October 2024.

— —/*Hanloser, Stefan/Weiß, Steffen,* 'PIMS im TTDSG Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz', European netID Foundation 2021.
— —/*Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (eds),* Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 3rd edn, Heidelberg 2024.

Schwartz, Ari, 'Looking Back at P3P: Lessons for the Future' (Center for Democracy & Technology, November 2009), https://cdt.org/wp-content/uploads/pdfs/P3P_Retro_Final_0.pdf, accessed 29 January 2026.
— —/*Sherry, Linda/Cooper, Mark/Tien, Lee/Pierce, Deborah/Brandt, Daniel/Smith, Rober Ellis/Givens, Beth/Dixon, Pam*, 'Consumer Rights and Protections in the Behavioral Advertising Sector', https://cdt.org/wp-content/uploads/privacy/20071031consumerprotectionsbehavioral.pdf, accessed 29 OctoberJanuary 2026.

Schwartz, Paul M., 'European Data Protection Law and Restrictions on International Data Flows', 80 Iowa L. Rev. 1995, 471-496.

Schweitzer, Heike/Peitz, Martin, 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?' [2018] 5 NJW 2018, 275-280.
— —/*Metzger, Axel/Blind, Knut/Richter, Heiko/Niebel, Crispin/Gutmann, Frederik*, Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy, Berlin 2022.
— —/*Metzger, Axel*, 'Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?', 4 GRUR Int. 2023, 337-356.

Schwemer, Sebastian Felix/Tomada, Letizia/Pasini, Tommaso, 'Legal AI Systems in the EU's Proposed Artificial Intelligence Act', in: Conrad, Jack G./Pickens, Jeremy (eds), Proceedings of the Second International Workshop on AI and Intelligent Assistance for Legal Professionals in the Digital Workspace (LegalAIIA 2021), Sao Paulo 2021, 1.

Science Europe, 'Practical Guide to the International Alignment of Research Data Management', Brussels 2021.

Scope, Nick/Rasin, Alexander/Wagner, James/Lenard, Ben/Heart, Karen, 'Purging Data from Backups by Encryption' in Strauss, Christine/Kotsis, Gabriele/Tjoa, Min A./Khalil, Ismail (eds), Database and Expert Systems Applications, Cham 2021, 245-158.

Scudiero, Lucio, 'Bringing Your Data Everywhere: A Legal Reading Of The Right To Portability', 3 EDPL 2017, 119-127.

Seiter, Stefan R., 'Auftragsverarbeitung nach der Datenschutz-Grundverordnung - Steuerberatertätigkeiten & andere Streitfragen – Ein kleiner Rundumschlag', 43 DuD 2019, 127-133.

Selbst, Andrew D./Powles Julia, 'Meaningful information and the right to explanation', 7 IDPL 2017, 233-242.

Sent, Esther-Mirjam, 'Rationality and bounded rationality: you can't have one without the other', 25 EJHET 2018, 1370-1386.

Sesing, Andreas, 'Cookie-Banner – Hilfe, das Internet ist kaputt! - Ansätze zur Verbesserung der Nutzererfahrung', 7 MMR 2021, 544-549.

Sharma, Shweta, 'European nations issue record €1.1 billion in GDPR fines', https://www.csoonline.com/article/571963/european-nations-issue-record-11-billion-in-gdpr-fines.html, 27 January 2022, accessed: 25 February 2026.

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (eds), Datenschutzrecht, 1st edn, Baden Baden 2019.

Simon, Herbert A., 'Bounded Rationality', in: Eatwell, John/Milgate, Murray/Newman, Peter (eds), Utility and Probability, 1st edn, London 1990, 15-18.

Singh, Jatinder/Cobbe, Jennifer, 'The Security Implications of Data Subject Rights', 17 IEEE S&P 2019, 21-30.

Sivathanu, Gopalan/Wright, Charles P./Zadok, Erez, 'Ensuring data integrity in storage: techniques and applications' in: Atluri, Vijay (ed) StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability, New York 2005, 26-36.

Slovic, Paul/Finucane, Melissa L./Peters, Ellen/MacGregor, Donald G., 'The affect heuristic', 177 Eur. J. Oper. Res. 2007, 1333-1352.

Snyder, Steven/Illman, Erin, 'Why some data subject request services create compliance concerns', https://iapp.org/news/a/why-some-dsr-services-create-compliance-concerns/, 23 March 2021, accessed: 22 February 2026.

Sobolčiaková, Angela, 'Right of Access under GDPR and Copyright' [2018] 12 MUJLT 2018, 221-246.

Soghoian, Christopher, 'The History of the Do Not Track Header', http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html, 21 January 2011, accessed: 25 February 2026.

Soh, Sheng Yin, 'Privacy Nudges: An Alternative Regulatory Mechanism to "Informed Consent" for Online Data Protection Behaviour', 5 EDPL 2019, 65-74.

Sommer, Martin, Haftung für autonome Systeme, 1st edn, Baden-Baden 2020.

Sørum, Hanne/Presthus, Wanda, 'Dude, Where's My Data? The GDPR in Practice, from a Consumer's Point of View', 34 Inf. Technol. People 2021, 912-929.

Specht, Louisa/Mantz, Reto (eds), Handbuch Europäisches und deutsches Datenschutzrecht, 1st edn, München 2019.

Specht-Riemenschneider, Louisa, 'Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch! - Überlegungen zur Anwendbarkeit der deliktischen Produzentenhaftung bei Inverkehrbringens datenschutzrechtlich relevanter Produkte', 2 MMR 2020, 73-78.

- — /*Schneider, Ruben*, 'Die gemeinsame Verantwortlichkeit im Datenschutzrecht - Rechtsfragen des Art. 26 DS-GVO am Beispiel "Facebook-Fanpages"', 8 MMR 2019, 503-509.
- —/*Schneider, Ruben*, 'Stuck Half Way: The Limitation of Joint Control after Fashion ID (EUGH Aktenzeichen C-40/17)', 2 GRUR Int. 2020, 159-163.
- — */Blankertz, Aline/Sierek, Pascal/Schneider, Ruben/Knapp, Jakob/Henne, Theresa*, 'Die Datentreuhand - Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle', 6 MMR-Beil 2021, 25-47.
- —, 'Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?', 5 ZRP 2022, 137-140.
- —, 'Der Entwurf des Data Act - Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G', MMR-Beilage 2022, 809-826.
- —/*Hennemann, Moritz (eds),* Data Governance Act, 1st edn, Baden-Baden 2023.

Spieker gen. Döhmann, Indra/Bretthauer, Sebastian, Dokumentation zum Datenschutz, 95th edn, Baden-Baden 2024.

Spindler, Gerald, 'Verschuldensunabhängige Produkthaftung im Internet', 3 MMR 1998, 119-124.
— —, 'Die neue EU-Datenschutz-Grundverordnung', 16 DB 2016, 937-947.
— —*/Schuster, Fabian (eds)*, Recht der elektronischen Medien, 4th edn, München 2019.
— —, 'User Liability and Strict Liability in the Internet of Things and for Robots', in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (eds), Liability for Artificial Intelligence and the Internet of Things, 1st edn, Baden-Baden 2019, 125-144.
— —, 'Klarheit für Cookies', 35 NJW 2020, 2513-2517.
— —, 'Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act (Teil 1)', 4 GRUR 2021, 545-553.
— —, 'Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz', 11 CR 2022, 689-704.
— —, 'Die Zukunft des europäischen Haftungsrechts für Internet-Provider – der Digital Services Act - Mögliche Auswirkungen auf die deutsche Rechtsprechung', 1 MMR 2023, 73-78.

Staunton, Ciara, 'Individual Rights in Biobank Research Under the GDPR', in: Slokenberga, Santa/Tzortzatou, Olga/Reichel, Jane (eds), GDPR and Biobanking, Cham 2021, 91-104.

Steinrötter, Björn (eds.), Europäische Plattformregulierung, 1st edn, Baden-Baden 2023.
— —, 'Verhältnis von Data Act und DS-GVO - Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung', 4 GRUR 2023, 216-226.

Steinsbekk, Kristin Solum/Myskja, Bjørn Kåre/Solberg, Berge, 'Broad Consent Versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem?', 21 Eur J Hum Genet 2013, 897-902.

Sterbenz, James P.G/Hutchison, David/Çetinkaya, Egemen K./Jabbar, Abdul/Rohrer, Justin P./Schöller, Marcus/Smith, Paul, 'Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines', 54 Comput. Netw. 2010, 1245.

Stock, Wolfgang G., 'N-ary Information Markets: Money, Attention, and Personal Data as Means of Payment', 8 JISTaP 2020, 6-14.

Stoklas, Jonathan, 'Videokameras in autonomen Fahrzeugen aus datenschutzrechtlicher Sicht', 15 ZD-Aktuell 2018, 06268.

Streich, Gregory W., 'Is There a Right to Forget? Historical Injustices, Race, Memory, and Identity', 24 New Political Science 2002, 525-542.

Strittmatter, Marc/Treiterer, Manuel/Harnos, Rafael, 'Schadensbemessung bei Datenschutzrechtsverstößen am Beispiel von data leakage-Fällen', 12 CR 2019, 789-797.

Strotz, RH, 'Myopia and Inconsistency in Dynamic Utility Maximization', 23 REStud 1995, 165-180.

Strowel, Alain, 'ChatGPT and Generative AI Tools: Theft of Intellectual Labor?' [2023] 54 IIC 2023, 491-494.

Strubel, Michael, 'Anwendungsbereich des Rechts auf Datenübertragbarkeit - Auslegung des Art. 20 DS-GVO unter Berücksichtigung der Guidelines der Art. 29-Datenschutzgruppe', 8 ZD 2017, 355-361.

Stürmer, Verena, 'Löschen durch Anonymisieren? - Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO', 12 ZD 2020, 626-631.

Sun, Tianshu/Yuan, Zhe/Li, Chunxiao/Zhang, Kaifu/Xu, Jun, 'The Value of Personal Data in Internet Commerce: A High-Stakes Field Experiment on Data Regulation Policy', 70 Management Science 2023, 2645-2660.

Sundar, Shyam S./Kim, Jinyoung/Rosson, Mary Beth/Molina, Maria D., 'Online Privacy Heuristics that Predict Information Disclosure', in: Bernhaupt, Regina/Mueller, Florian/Verweij, David/Andres Josh (eds), Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, New York 2020, 1-12.

Sunstein, Cass R., 'Nudges, Agency, and Abstraction: A Reply to Critics', 6 Rev. Philos. Psychol. 2015, 511-529.

Sunyaev, Ali/Dehling, Tobias/Taylor, Patrick L./Mandl, Kenneth D, 'Availability and quality of mobile health app privacy policies', 22 JAMIA 2015, e28-33.

Sury, Ursula, 'Pflichten im Auftragsverarbeitungsverhältnis', 44 Informatik Spektrum 2021, 376-378.

Swire, Peter/Lagos, Yianni, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', 72 Md. L. Rev. 2013, 335-380.

Sydow, Gernot/Marsch, Nikolaus (eds), Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 3rd edn, Baden-Baden 2022.

Sykes, Charles J., The End of Privacy: The Attack on Personal Rights at Home, at Work, Online, and in Court, 1st edn, New York 1999.

Szczepański, Marcin, 'Briefing: Is data the new oil? - Competition issues in the digital economy', European Union 2020.

Tabassum, Madiha/Alqhatani, Abdulmajeed/Aldossari, Marran/Richter Lipford, Heather, 'Increasing User Attention with a Comic-based Policy', in: Mandryk, Regan/Hancock, Mark (eds.), Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, New York 2018.

Taeger, Jürgen, 'Einwilligung von Kindern gegenüber Diensten der Informationsgesellschaft - Schutz von Kindern unter 16 Jahren durch Art. 8 DS-GVO vor Beeinträchtigungen im Netz', 9 ZD 2021, 505-508.

— *—/Gabel, Detlev (eds)*, DSGVO-BDSG-TTDSG, 4th edn, Frankfurt am Main 2022.

Tang, Qiang, 'Timed-Ephemerizer: Make Assured Data Appear and Disappear' in: Martinelli, Fabio/Preneel, Bart (eds), Public Key Infrastructures, Services and Applications, Heidelberg 2010, 195-208.

— —, 'From Ephemerizer to Timed-Ephemerizer: Achieve Assured Lifecycle Enforcement for Sensitive Data', 58 Comput. J. 2015, 1003-1020.

Tang, Yang/Lee, Patrick P.C./Lui, John C.S./Perlman, Radia, 'FADE: Secure Overlay Cloud Storage with File Assured Deletion' in: Jajodia, Sushil/Zhou, Jianying (eds), Security and Privacy in Communication Networks, Heiderlberg 2010, 380-397.

Taylor, David G./Davis, Donna F/Jillapalli, Ravi, 'Privacy concern and online personalization: The moderating effects of information control and compensation', 9 JECR 2009, 203-223.

Teare, Harriet J A/Hogg, Joanna/Kaye, Jane/Luqmani, Raashid/Rush, Elaine/Turner, Alison/Watts, Laura/Williams, Melanie/Javaid, M Kassim, 'The RUDY Study: Using Digital Technologies to Enable a Research Partnership', 25 Eur J Hum Genet 2017, 816-822.

— —/*Prictor, Megan/Kaye, Jane*, 'Reflections on Dynamic Consent in Biomedical Research: The Story So Far', 29 Eur J Hum Genet 2021, 649-565.

Teevan, Jaime/Jones, William/Bederson, Benjamin B., 'Session details: Personal information management' [2006] 49 Commun. ACM 2006, 40.

ten Teije, Stefan, 'First-party cookies: "Get legal help to avoid fines", https://www.journalism.co.uk/news/first-party-cookies-get-legal-help-to-avoid-fines-/s2/a982617/, 14 November 2022, accessed: 25 February 2025.

Tene, Omar/Polonetsky, Jules, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', 13 Minn. J.L. Sci. & Tech. 2012, 281-357.

Terhechte, Jörg Philipp (ed), Verwaltungsrecht der Europäischen Union, 2nd edn, Nomos 2022.

Tesfay, Welderufael B./Hofmann, Peter/Nakamura, Toru/Kiyomoto, Shinsaku/Serna, Jetzabel, 'PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation' in Verma, Rakesh/Katarcioglu, Murat (eds), IWSPA '18: Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, New York 2018, 15-21.

Thaler, Richard, 'Some empirical evidence on dynamic inconsistency', 8 Econ. Lett. 1981, 201-207.

— —/*Sunstein, Cass R.*, Nudge: Improving Decisions about Health, Wealth and Happiness, 1st edn, New Haven 2008.

Thibault, Jaymi, Evaluating the Impact of the GDPR's Data Subject Rights on Businesses, Master Thesis, Sanford 2021.

Thiel, Barbara/Wybitul, Tim, Bußgelder wegen Datenschutzverstößen – aus Sicht von Aufsichtsbehörden und Unternehmen, 1 ZD 2020, 3-7.

Thode, Jan-Christoph, 'Die neuen Compliance-Pflichten nach der Datenschutz- Grundverordnung', 11 CR 2016, 714-721.

Thöne, Meik, Autonome Systeme und deliktische Haftung, 1st edn, Tübingen 2020.

Tian, Xinluan/Chen, Lina/Zhang, Xiaojuan, 'The Role of Privacy Fatigue in Privacy Paradox: A PSM and Heterogeneity Analysis' [2022] 12 Applied Sciences 2022, 9702.

Ticher, Paul, Data Protection vs Freedom of Information: Access and Personal Data, 1st edn., Cambridgeshire 2008.

Tolmie, Peter/Crabtree, Andy/Rodden, Tom/Colley, James/Luger, Ewa, '"This Has to Be the Cats": Personal Data Legibility in: Networked Sensing Systems' in Gergle, Darren/Ringel Morris, Meredith (eds), CSCW '16: Proceedings of the

19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, San Francisco 2016, 491-502.

Trentmann, Christian, 'Das „Recht auf Vergessenwerden“ bei Suchmaschinentrefferlinks', 33 CR 2017, 26-35.

Triaille, Jean-Paul, 'The EEC Directive of July 25, 1985 on liability for defective products and its application to computer programs', 9 CLSR. 1993, 214-226.

Turle, Marcus, 'Freedom of information and the public interest test', 23 2007, CLSR 167-176.

Tversky, Amos/Kahneman, Daniel, 'On the psychology of prediction', 80 Psychological Review 1973, 237-251.

- —/*Kahneman, Daniel*, 'Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty', 185 Science 1974, 1124-1131.
- —/*Kahneman, Daniel*, 'The Framing of Decisions and the Psychology of Choice', 211 Science 1981, 453-457.

Twigg-Flesner, Christian, 'The Tale of the Grating Horseradish – Case Note on KRONE-Verlag (C-65-20)', 10 EuCML 2021, 262-265.

Ulmenstein, Ulrich Frhr. von, ‘Datensouveränität durch repräsentative Rechtswahrnehmung - Begriffliche Prägung und normative Gestaltung sogenannter „Datentreuhänder“’, 44 DuD 2020, 528-534.

University of Southampton, 'Research Data Management Policy', https://www.southampton.ac.uk/about/governance/regulations-policies/policies/research-data-management, June 2024, last accessed: 17 February 2026.

Ur, Blasé/Leon, Pedro Giovanni/Cranor, Lorrie Faith/Shay, Richard/Wang, Yang, ‘Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising’ in Cranor, Lorrie Faith (ed), SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security, New York 2012, 1-15.

Urban, Tobias/Tatang, Dennis/Degeling, Martin/Holz, Thorsten/Pohlmann, Norbert, 'The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR', https://arxiv.org/abs/1811.08660v1, 21 November 2018, accessed: 02 March 2026.

- —/*Tatang, Dennis/Degeling, Martin/Holz, Thorsten/Pohlmann, Norbert*, 'A Study on Subject Data Access in Online Advertising After the GDPR'

in: Pérez-Solà, Cristina/Navarro-Arribas, Guillermo/Biryukov, Alex/Garcia-Alfaro, Joaquin (eds.), Data Privacy Management, Cryptocurrencies and Blockchain Technology, Cham 2019, 61-79.

Urquhart, Lachlan/Sailaja, Neelima/McAuley, Derek, 'Realising the right to data portability for the domestic Internet of things', 22 Pers Ubiquit Comput 2018, 317-332.

— *—/Lodge, Tom/Crabtree, Andy*, 'Demonstrably doing accountability in the Internet of Things', 27 Int. J. Law Inf. Technol. 2019, 1-27.

Ursic, Helena, 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control', 15 SCRIPTed 2018, 42-69.

Ustaran, Eduardo (ed), European Data Protection Law and Practice, 2nd edn, Portsmouth 2019.

Utz, Christine/Degeling, Martin/Fahl, Sascha/Schaub, Florian/Holz, Thorsten, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' in Cavallaro. Lorenzo/Kinder, Johannes (eds), CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, New York, 973-990.

Van Alsenoy, Brendan, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', 7 JIPITEC 2016, 271-288.

Van der Auwermeulen, Barbara, 'How to attribute the right to data portability in Europe: A comparative analysis of legislations', 33 CLSR 2017, 57-72.

van Ooijen, I./Vrabec, Helena U., 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective', 42 J Consum Policy 2019, 91-107.

van Raay, Anne/Meyer-van Raay, Oliver, 'Opt-in, Opt-out und (k)ein Ende der Diskussion', 3 VuR 2009, 103-109.

Vanberg, Aysem Diker/Ünver, Mehmet Bilal, 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' [2017] 8 EJLT 2017, 1-22.

Vander Maelen, Carl, 'Codes of (Mis)Conduct? An Appraisal of Articles 40-41 GDPR in View of the 1995 Data Protection Directive and Its Shortcomings', 6 EDPL 2020, 231-242.

Vardanyan, Lusine / Kocharyan, Hovsep, 'The GDPR and the DGA Proposal: are They in Controversial Relationship?', 9 Eur. Stud. 2022, 91 - 109.

Veale, Michael/Binns, Rreuben/Ausloos, Jef, 'When data protection by design and data subject rights clash', 8 IDPLaw 2018, 105-123.

Veldt, Gitta, 'The New Product Liability Proposal – Fit for the Digital Age or in Need of Shaping Up? - An Analysis of the Draft Product Liability Directive', 1 EuCML 2023, 24-31.

Verbraucherzentrale Bundesverband e.V., 'Neue Datenintermediäre - Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder', https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf, 15. September 2020, accessed: 25 Februar 2025.

Vidhani, Kumar/Banahatti, Vijayanand/Lodha, Sachin, 'Challenges in enabling privacy self management', 9 CSIT 2021, 185-191.

Vladeck, Stephen I., 'Expert Opinion on the Current State of U.S. Surveillance Law and Authorities', Bonn 2021.

Voigt, Paul, 'Datenschutz bei Google', 6 MMR 2009, 377-382.

— *—/von dem Bussche, Axel*, The EU General Data Protection Regulation (GDPR), 1st edn, Cham 2017.

Voit, Karl/Andrews, Keith/Slany, Wolfgang, 'Why Personal Information Management (PIM) Technologies Are Not Widespread´, in: Personal information intersections: What happens when PIM spaces overlap?, Vancouver 2009, 60-64.

Völker, Jan Christoph/Schnatz, Andreas/Breyer, Jonas, 'Chancen und Risiken von Cloud-Produkten im Unternehmen - Cloud Computing – mehr als nur SaaS', 6 MMR 2022, 427-435.

von Ditfurth, Lukas/Lienemann, Gregor, 'The Data Governance Act: Promoting or Restricting Data Intermediaries?', 23 CRNI 2022, 270-295.

von Grafenstein, Maximilian/Heumüller, Julia/Belgacem, Elias/Jakobi, Timo/Smieskol, Patrick, 'Effective Regulation through Design – Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection by Design Approach', Berlin 2021.

von Paczinsky und Tenczin, Kristina, Who is the controller for data processing and who is the processor?, https://www.datenschutz-notizen.de/who-is-the-controller-for-data-processing-and-who-is-the-processor-2727529/, 19 October 2020, accessed: 03 March 2026.

Wachter, Sandra/Mittelstadt, Brent/Floridi, Luciano, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 7 IDPL 2017, 76-99.

Wagner, Bernd, 'Disruption der Verantwortlichkeit - Private Nutzer als datenschutzrechtliche Verantwortliche im Internet of Things', 7 ZD 2018, 307-312.

Wagner, Gerhard, 'Liability Rules for the Digital Age – Aiming for the Brussels Effect', 13 JETL 2022, 191-243.

Waldman, Ari Ezra, 'Cognitive Biases, Dark Patterns, and the "Privacy Paradox"', 31 Current Opinion in Psychology 2020, 105-109.

Walker, Robert, 'The Right to be Forgotten' 64 Hastings L.J. 2012, 257-286.

Wandtke, Arthur-Axel, 'Ökonomischer Wert von persönlichen Daten – Diskussion des „Warencharakters" von Daten aus persönlichkeits- und urheberrechtlicher Sicht', 1 MMR 2017, 6-12.

Wang, Xiaoyin/Qin, Xue/Hosseini, Mitra Bokaei/Slavin, Rocky/Breaux, Travis D./Niu, Jianwei, 'GUILeak: Identifying Privacy Practices on GUI-Based Data', https://cdn.stmarytx.edu/wp-content/uploads/2020/10/GUILeak-Identifying-Privacy-Practices-on-GUI-Based-Data.pdf, accessed: 25 February 2026.

Wang, Yang/Norcie, Gregory/Komanduri, Saranga/Acquisti, Alessandro/Leon, Pedro Giovanno/Cranor, Lorrie Faith, '"I Regretted the Minute I Pressed Share": A Qualitative Study of Regrets on Facebook', in Cranor, Lorrie Faith (ed), SOUPS '11: Symposium on Usable Privacy and Security, New York 2011, 1-16.

Weber, Rolf H., 'The Right to Be Forgotten More Than a Pandora's Box?', 2 JIPITEC 2011, 119-130.

Wedde, Peter, 'Automatisierung im Personalmanagement – arbeitsrechtliche Aspekte und Beschäftigtendatenschutz', Berlin 2020.

Weichert, Thilo, 'Kein Patientengeheimnis bei ärztlichen Haftpflichtverfahren?', 4 VuR 2017, 138-142.

— —, 'Verantwortlichkeiten bei Social-Media-Plattformen', 42 DANA 2019, 4-10.

— —, ‘Die Forschungsprivilegierung in der DS-GVO - Gesetzlicher Änderungsbedarf bei der Verarbeitung personenbezogener Daten für Forschungszwecke’, 1 ZD 2020, 18-24.
— —, 'Datenschutz und Mitbestimmung in Matrixorganisationen - Schutz von Beschäftigtendaten bei externer Verarbeitung', 1 NZA 2023, 13-21.

Weinmann, Markus / Schneider, Christoph / vom Brocke, Jan, 'Digital Nudging', 58 Bus Inf Syst Eng 2016, 433 - 436.

Weinstein, Neil D./Klein, William MP, 'Unrealistic Optimism: Present and Future', 15 J. Soc. Clin. Psychol. 1996, 1-8.

Wendehorst, Christiane/Graf von Westphalen, Friedrich, ‘Das Verhältnis Zwischen Datenschutz-Grundverordnung und AGB-Recht’, 52 NJW 2016, 3745-3751.

Wernick, Alina, 'Defining Data Intermediaries - A Clearer View Through the Lens of Intellectual Property Governance', 2 TechReg 2020, 65-81.

Werro, Franz, 'The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash', in: Colombi Ciacchi, Aurelia/Godt, Christine/Rott, Peter/Smith, Lesley Jane (eds), Haftungsrecht im dritten Millennium - Liability in the Third Millennium, 1st edn, Baden-Baden 2009, 285.
— —, 'The Right to Be Forgotten: The General Report—Congress of the International Society of Comparative Law, Fukuoka, July 2018', in: Werro, Franz (ed), The Right To Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia, 1st edn, Cham 2020, 1-35.

Wessels, Michael, 'Schmerzensgeld bei Verstößen gegen die DSGVO', 43 DuD 2019, 781.

Westphal, Dietrich, ‘Die Neue EG-Richtlinie zur Vorratsdatenspeicherung - Privatsphäre und Unternehmerfreiheit unter Sicherheitsdruck’, 18 EuZW 2006, 555-560.

WHO, Code of Conduct for responsible Research, November 2017.

Whittaker, Steve/Jones, Quentin/Nardi, Bonnie/Creech, Mike/Terveen, Loren/Isaacs, Ellen/Hainsworth, John, 'ContactMap: Organizing communication in a social desktop', 11 ACM Trans. Comput.-Hum. Interact. 2004, 445-471.
—, *—/Bellotti, Victoria/Gwizdka, Jacek*, 'Email in personal information management', 49 Commun. ACM 2006, 68-73.

Wichtermann, Marco, 'Einführung eines Datenschutz-Management-Systems im Unternehmen – Pflicht oder Kür? - Kurzüberblick über die Erweiterungen durch die DS-GVO', 9 ZD 2016, 421-422.

Wiebe, Andreas, 'The Data Act Proposal - Access rights at the Intersection with Database Rights and Trade Secret Protection', 4 GRUR 2023, 227 - 238.

Winter, Christian/Battis, Verena/Halvani, Oren, 'Herausforderungen für die Anonymisierung von Daten - Technische Defizite, konzeptuelle Lücken und rechtliche Fragen bei der Anonymisierung von Daten', 11 ZD 2019, 489-492.

Wirth, Thomas, 'Die Pflicht zur Löschung von Forschungsdaten – Urheber- und Datenschutzrecht im Widerspruch zu den Erfordernissen guter wissenschaftlicher Praxis?', 8 ZUM 2020, 585-592.

Wolff, Heinrich Amadeus, 'Verhaltensregeln nach Art. EWG_DSGVO Artikel 40 DS-GVO auf dem Prüfstand - Neuauflage eines europäischen Instituts mit schlechter Entwicklungsprognose', 4 ZD 2017, 151-154.

- *—/Brink, Stefan/von Ungern-Sternberg, Antje*, BeckOK Datenschutzrecht, 49th edn, München 2024.

Wuyts, Daily, 'The Product Liability Directive – More than two Decades of Defective Products in Europe', 5 JETL 2014, 1-34.

Wybitul, Tim (ed), Handbuch: EU-Datenschutz-Grundverordnung, 1st edn., Frankfurt am Main 2017.

- *—/Neu, Leonie/Strauch, Martin*, 'Schadensersatzrisiken für Unternehmen bei Datenschutzverstößen - Verteidigung gegen Schadensersatzforderungen nach Art. 82 DS-GVO' [2018] 5 ZD 2018, 202-207.
- *—/Haß, Detlef/Albrecht, Jan Philipp,* 'Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung', 3 NJW 2018, 113-118.
- *—/Brams, Isabelle*, 'Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 Absatz I DS-GVO? - Zugleich eine Analyse des Urteils des LAG Baden-Württemberg vom 20.12.2018', 10 NZA 2019, 672-677.
- *—/Leibold, Kevin,* 'Risiken für Unternehmen durch neue Rechtsprechung zum DS-GVO-Schadensersatz - Ein Überblick über die Voraussetzungen und die aktuelle Rechtsprechung zu Art. 82 DS-GVO', 4 ZD 2022, 207-215.

Xiang, Su/Hyysalo, Jarkko/Rautiainen, Mika/Riekki, Jukka/Sauvola, Jaakk/Maarala, Altti Ilari/Hirvonsalo, Harri/Li, Pingjiang/Honko, Harri, 'Privacy as

a Service: Protecting the Individual in Healthcare Data Processing', 49 Computer 2016, 49-59.

Yang, Pan/Xiong, Naixue/Ren, Jingli, 'Data Security and Privacy Protection for Cloud Storage: A Survey', 8 IEEE Access 2020, 131723, 131724.;

Zalnieriute, Monika/Churches, Genna, 'When a "Like" Is Not a "Like": A New Fragmented Approach to Data Controllership', 83 MLR 2020, 861-876.

Zanfir, Gabriela, 'The right to Data portability in the context of the EU data protection reform', 2 IDPL 2012, 149-162.

Zarras, Apostolis/Kohls, Katharina/Dürmuth, Markus/Pöpper, Christina, 'Neuralyzer: Flexible Expiration Times for the Revocation of Online Data', in: Bertino, Elisa/Sandhu, Ravi (eds.) Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy (Association for Computing Machinery 2016) 14-25.

Zech, Herbert, Information als Schutzgegenstand, 1st edn, Tübingen 2012.

— —, Gutachten A zum 73. Deutschen Juristentag - Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, 1st edn, München 2020.

— —, 'Liability for AI: public policy considerations', 22 ERA Forum 2021, 147-158.

Zhou, Lei/Fu, Anmin/Yu, Shui/Su, Mang/Kuang, Boyu, 'Data integrity verification of the outsourced big data in the cloud environment: A survey', 122 JNCA 2018, 1-15.

Ziegenhorn, Gero/Fokken, Martin, 'Rechtsdienstleister: Verantwortliche oder Auftragsverarbeiter? - Rechtsanwälte und Inkassounternehmen als Adressaten der DS-GVO', 5 ZD 2019, 194-199.

Zikesch, Philipp/Sörup, Thorsten, 'Der Auskunftsanspruch nach Art. 15 DS-GVO - Reichweite und Begrenzung', 6 ZD 2019, 239-245.

Zimmeck, Sebastian/Wang, Ziqi/Zou, Lieyong/Iyengar, Roger/Liu, Bin/Schaub, Florian/Wilson, Shomir/Sadeh, Norman/Bellovin, Steven M./Reidenberg, Joel, 'Automated Analysis of Privacy Requirements for Mobile Apps', NDSS Symposium, San Diego 2017.

— *—/Story, Peter/Smullen, Daniel/Ravichander, Abhilasha/Wang, Ziqi/Reidenberg, Joel/Russell, N. Cameron/Sadeh, Norman*, 'MAPS: Scaling Privacy Compliance Analysis to a Million Apps', PoPETs 2019, 66-86.

Zimmer, Daniela, 'Streamingplattformen im Datenschutz-Test: Wie transparent informieren Onlineanbieter von Musik und Videos ihre Kunden über die Verwendung ihrer Daten?', Wien 2020.

Zimmermann, Christian, 'A Categorization of Transparency-Enhancing Technologies', Amsterdam Privacy Conference 2015.

Zittrain, Jonathan, The Future of the Internet—And How to Stop It, New Haveven & London 2009.

Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 1st edn, New York 2019.

Zucker-Scharff, Aram/Zimmeck, Sebastian, 'How to Implement Global Privacy Control (GPC) for Publishers', https://globalprivacycontrol.org/Implementing%20GPC%20for%20Publishers.pdf, accessed: 25 February 2026.

Zuiderveen Borgesius, Frederik/Helberger, Natali/Reyna, Agustin, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law', 54 CMLRev 2017, 1427-146

digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Janina Rochon

Questionable Control.

The thesis examines PIMS with regard to the unresolved allocation of responsibility and liability under the GDPR. It identifies that the roles allocated under the GDPR are often inconsistent and analyses the resulting risks. In the final part, various approaches to resolving the identified issues are proposed.