digital | recht

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

Charlotte Schindler

Zulässigkeit und Grenzen algorithmischer Systeme bei arbeitsrechtlichen Auswahlentscheidungen

Eine rechtliche Betrachtung der Einsatzmöglichkeiten algorithmischer Systeme mit Fokus auf die DSGVO, das AGG und eine zukünftige KI-VO

Band 16

Charlotte Schindler

Zulässigkeit und Grenzen algorithmischer Systeme bei arbeitsrechtlichen Auswahlentscheidungen

Eine rechtliche Betrachtung der Einsatzmöglichkeiten algorithmischer Systeme mit Fokus auf die DSGVO, das AGG und eine zukünftige KI-VO

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 16

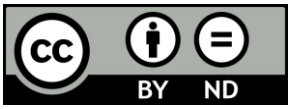
Charlotte Schindler; geboren 1996; Rechtsreferendarin und wissenschaftliche Mitarbeiterin am Zentrum für Juristisches Lernen der Bucerius Law School in Hamburg; Studium der Rechtswissenschaften in Hamburg und Lyon; 2019 Erste Juristische Prüfung.

ORCID: 0009-0000-5122-7668

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: 9783758428401
URN: urn:nbn:de:hbz:385-2023120707
DOI: https://doi.org/10.25353/ubtr-ad99-7ffe-3dab



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

Für meine Eltern und Moritz

Vorwort

Der Promotionsausschuss der Bucerius Law School, Hochschule für Rechtswissenschaft, Hamburg, hat diese Arbeit im August 2023 als Dissertation angenommen. Die mündliche Prüfung fand am 12. Dezember 2023 statt. Rechtsprechung und Literatur habe ich zuletzt im November 2023 aktualisiert.

Bedanken möchte ich mich zunächst bei meinem Doktorvater *Professor Dr. Matthias Jacobs*, der mich während der Promotionszeit an seinem Lehrstuhl gefördert und gefordert hat. Das Vertrauen, das er mir entgegengebracht hat, weiß ich sehr zu schätzen. Die Zeit am Lehrstuhl war lehrreich und in jeder Hinsicht – sowohl fachlich als auch persönlich – bereichernd.

Professor Dr. Michael Kort danke ich herzlich für die zügige Erstellung des Zweitgutachtens. Bei *Professor Dr. Benjamin Raue* sowie den weiteren Herausgeberinnen möchte ich mich für die Aufnahme in die Schriftenreihe „digital | recht – Schriften zum Immaterialgüter-, IT-, Medien-, Daten- und Wettbewerbsrecht“ bedanken.

Hervorheben möchte ich außerdem die *Law & AI Research Group*, bei deren Aufbau ich mitwirken durfte. Die Organisation verschiedener Veranstaltungen rund um das Thema „KI und Recht“ hat mir große Freude bereitet. Der daraus resultierende Austausch mit anderen Promovierenden war stets hilfreich und vor allem auch motivierend. Insbesondere möchte ich *Dr. Sophie Burchardi* danken, die mich mit ihrer Begeisterung und ihrem Engagement für wissenschaftliche Veranstaltungen angesteckt hat.

Außerdem möchte ich mich bei allen bedanken, die Teile der Arbeit Korrektur gelesen haben. Namentlich hervorheben möchte ich *Michael Nickel*, der die

Arbeit sowohl bei der Vor- als auch bei der Endabgabe mit großer Genauigkeit gelesen hat.

Bei meinen Eltern, *Iris* und *Wolfgang Schindler* möchte ich mich dafür bedanken, dass sie mich immer bedingungslos unterstützen und ich mich jederzeit auf sie verlassen kann.

Schließlich bin ich überaus dankbar, dass ich auch Herausforderungen wie das Schreiben einer Dissertation mit *Moritz Nickel* teilen kann. Mit seinen kritischen Nachfragen und der Fähigkeit, immer die richtigen motivierenden Worte zu finden, hat er maßgeblich zur Entstehung dieser Arbeit beigetragen. Ihm und meinen Eltern widme ich diese Arbeit.

Hamburg, im Dezember 2023 *Charlotte Schindler*

Inhaltsverzeichnis

Vorwort V
Inhaltsverzeichnis VII
Abkürzungsverzeichnis XXIII
Einleitung 1
Gang der Untersuchung 5

Teil 1
Algorithmische Systeme im Kontext arbeitsrechtlicher Auswahlentscheidungen 7

Kapitel 1
Begriffsbestimmung und technische Grundlagen 9
A. Algorithmische Systeme 9
B. Klassische Algorithmen und Lernalgorithmen 10
C. Maschinelles Lernen als Teilgebiet von KI 12
I. Lernstile 15
1. Überwachtes Lernen 15
2. Unüberwachtes Lernen 16
3. Verstärkendes Lernen 16
II. Künstliche neuronale Netze 17
1. Aufbau eines künstlichen neuronalen Netzes 18
2. Lernprozess des neuronalen Netzes 19
D. Zwischenergebnis: Algorithmische Systeme im Kontext dieser Arbeit ... 20

Kapitel 2
Anwendungsszenarien 23
A. Bewerbungsverfahren 24
I. *Recommender-Systeme* bei Karrierenetzwerken 24

II. Chatbots ... 25
III. Persönlichkeitsbewertung mithilfe von Video- oder Sprachanalysen ... 26
IV. *„Background-Checks"* mithilfe algorithmischer Systeme ... 28
B. Beförderung ... 29
I. Interne Bewerbungsprozesse ... 29
II. Leistungsbewertungssysteme ... 30
C. Kündigung ... 31
D. Zwischenergebnis: Kein flächendeckender Einsatz in Deutschland ... 32

Kapitel 3
Menschliche und algorithmische Entscheidungen im Vergleich ... 33
A. Objektivität und Determiniertheit ... 33
B. Auswertung großer Datenmengen ... 35
C. Keine Berücksichtigung individueller Merkmale und Korrelation ... 36
D. Zwischenergebnis: Vor- und Nachteile sowohl menschlicher als auch algorithmischer Entscheidungen ... 38

Kapitel 4
Transparenz als zentrales Element für mehr Vertrauen ... 39
A. Ursachen für Intransparenz von maschinell lernenden Systemen ... 40
I. Technische und rechtliche Hürden ... 40
1. Technische Intransparenz ... 40
2. Rechtliche Intransparenz ... 41
II. *Explainable AI* ... 42
B. Nutzen von Transparenz und Mindestanforderungen ... 44
I. Transparenz als Oberbegriff für Nachvollziehbarkeit und Erklärbarkeit ... 45
II. Relevante Auslegungsaspekte ... 46
III. Nutzen von Transparenz ... 46
C. Zwischenergebnis: Zwei Bestandteile des Transparenzbegriffs ... 47

Teil 1
Zusammenfassung ... 49

Teil 2
Datenschutzrechtliche Anforderungen an algorithmische Systeme 51

Kapitel 5
Überblick über die rechtlichen Rahmenbedingungen 53
A. Unions- und völkerrechtliche Vorgaben 53
I. Anwendungsvorrang des Unionsrechts 53
II. Zusammenspiel von Art. 8 EMRK, Art. 16 AEUV, Art. 7 und 8 GRCh 54
1. Verhältnis von Art. 8 EMRK, Art. 16 AEUV, Art. 7 und 8 GRCh 55
a) EMRK als Rechtserkenntnisquelle 56
b) Grundrechtsbindung Privater 58
2. Art. 7, 8 GRCh als maßgebliches Datenschutzgrundrecht 60
3. Schutzbereich von Art. 7, 8 GRCh 60
a) Sachlicher Schutzbereich 60
b) Persönlicher Schutzbereich 61
III. DSGVO als maßgebliche Verordnung für den Schutz personenbezogener Daten 61
1. Auslegung der DSGVO 62
a) Art. 29-Datenschutzgruppe 63
b) Europäischer Datenschutzausschuss 63
c) Datenschutzkonferenz 64
2. Anwendungsbereich der DSGVO 65
a) Sachlicher Anwendungsbereich 65
aa) Personenbezogene Daten 65
(1) Informationen 66
(2) Identifizierte oder identifizierbare Person 68
(3) Ganz und teilweise automatisierte Verarbeitung 68
bb) Nichtautomatisierte Verarbeitung 69
b) Persönlicher Anwendungsbereich 70
c) Räumlicher Anwendungsbereich 70
aa) Niederlassungsprinzip 70
bb) Marktortprinzip 71
cc) Völkerrecht 73
3. Zwischenergebnis: weiter Anwendungsbereich der DSGVO 73

IV. KI-VO: Regulierung von KI auf unionaler Ebene 74
1. Hintergrund und Stand des Gesetzgebungsverfahrens 74
2. Verhältnis einer zukünftigen KI-VO zur DSGVO 76
3. Anwendungsbereich einer zukünftigen KI-VO 77
a) Sachlicher Anwendungsbereich einer zukünftigen KI-VO 77
b) Persönlicher und räumlicher Anwendungsbereich einer zukünftigen KI-VO 79
4. Ziele einer zukünftigen KI-VO 80
5. Risikobasierter Ansatz einer zukünftigen KI-VO 82
6. Zwischenergebnis: Algorithmische Systeme von einer zukünftigen KI-VO erfasst 82
V. KI-HaftRL-E 84
1. Gesetzgeberischer Hintergrund 84
2. Inhalt des KI-HaftRL-E 84
3. Bedeutung des KI-HaftRL-E für den Untersuchungsgegenstand 85
B. Nationale Ebene 85
I. Recht auf informationelle Selbstbestimmung 86
1. Sachlicher Schutzbereich 86
2. Persönlicher Schutzbereich 86
II. Einfachgesetzliche Grundlagen 87
1. Verhältnis des § 26 BDSG zu den Vorschriften der DSGVO 87
a) § 26 Abs. 1 S. 1 BDSG als „spezifischere Vorschrift“ i. S. d. Art. 88 Abs. 1 DSGVO? 89
b) § 26 Abs. 1 S. 1 BDSG erfüllt nicht die Anforderungen von Art. 88 Abs. 1 und 2 DSGVO 90
c) § 26 Abs. 1 S. 1 BDSG ist unanwendbar 92
d) § 26 BDSG ist im Übrigen weiterhin anwendbar 92
2. Datenschutz im BetrVG 93
3. Abgrenzung zum TMG/TKG/TTDSG 94
D. Zwischenergebnis: Folgen für algorithmische Systeme 95

Kapitel 6
Rechtmäßigkeit der Datenverarbeitung 97
A. Generelle Anforderungen an die Rechtmäßigkeit der Datenverarbeitung 98

I. Verantwortlichkeit für die Datenverarbeitung 99
1. Datenschutzrechtlich Verantwortliche 99
2. Einsatz von algorithmischen Systemen als Variante der der gemeinsamen Verantwortlichkeit oder der Auftragsverarbeitung .. 99
a) Gemeinsame Verantwortliche 99
b) Auftragsverarbeitung 101
c) Rechtsfolgen 102
3. Benennung einer Datenschutzbeauftragten 103
II. Erfordernis einer Rechtsgrundlage 104
1. Art. 6 DSGVO als zentrale Vorschrift 104
a) Überblick über Art. 6 DSGVO 104
b) Art. 9 DSGVO als zusätzliche Voraussetzung neben Art. 6 DSGVO 105
c) Sperrwirkung gegenüber Art. 6 Abs. 1 S. 1 lit. f DSGVO 107
d) Zweckänderung nach Art. 6 Abs. 4 DSGVO möglich 107
2. Art. 6 Abs. 1 S. 1 lit. b DSGVO als Rechtsgrundlage bei der Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis 108
a) § 26 Abs. 1 S. 1 BDSG als unanwendbare Vorschrift 108
b) Keine Sperrwirkung gegenüber den anderen Erlaubnistatbeständen des Art. 6 DSGVO 108
c) § 26 Abs. 3 S. 1 BDSG als Umsetzung von Art. 9 Abs. 2 lit. b DSGVO 109
III. Nebeneinander von Rechtfertigungstatbeständen: Verarbeitung nach Wegfall einer Rechtsgrundlage 110
1. Wortlaut von Art. 6 und 17 DSGVO 111
2. Ansichten in der Literatur und der Rechtsprechung 111
3. Ansicht der Art. 29-Datenschutzgruppe und des EDSA 112
4. Fazit: Nebeneinander von Rechtsgrundlagen möglich 113
IV. Verbindlichkeit der Datenschutzgrundsätze 114
V. Zwischenergebnis: generelle Anforderungen an die Rechtmäßigkeit 115
B. Training maschinell lernender Systeme 117
I. Technische Möglichkeiten zur Anonymisierung 118
1. Generalisierung 118
2. Randomisierung 119

3. Anonymisierungstechniken bei Video-/Tonaufnahmen 120
II. Ausschluss des Personenbezugs durch Anonymisierung 121
1. Abgrenzung zur Pseudonymisierung 121
2. Anonymisierende Wirkung der Pseudonymisierung 122
3. Rechtliche Zulässigkeit der Anonymisierung 123
a) Art. 6 Abs. 1 S. 1. lit. f DSGVO 123
aa) Anwendungsbereich 124
bb) Berechtigte Interessen 124
cc) Maßstab der Erforderlichkeit 125
dd) Erforderlichkeit und entgegenstehende Interessen 126
b) Rechtsgrundlage für die Verarbeitung sensibler Daten 127
c) Art. 6 Abs. 1 S. 1 lit. c DSGVO i. V. m. Art. 17 DSGVO 129
4. Zwischenergebnis: wirksame Anonymisierung schwierig umsetzbar 131
III. Synthetische Daten als Alternative zur Anonymisierung 131
IV. Training maschinell lernender Systeme als Zweckänderung gem. Art. 6 Abs. 4 DSGVO 133
1. Art. 6 Abs. 4 DSGVO als eigenständige Rechtsgrundlage 133
2. Einwilligung 135
3. Art. 54 Abs. 1 KI-VO-KOM 137
4. Voraussetzungen des Kompatibilitätstests in Art. 6 Abs. 4 DSGVO 137
a) Maßstab 138
b) Verbindung der Zwecke beim Training maschinell lernender Systeme 140
c) Art der personenbezogenen Daten 141
d) Folgen der Weiterverarbeitung für die betroffene Person 141
e) Vorhandensein geeigneter Garantien 142
f) Zwischenergebnis: hohe Anforderungen des Kompatibilitätstests 144
V. Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO 145
1. Formelle Voraussetzungen 146
2. Materielle Voraussetzungen 146
a) Freiwilligkeit als zentrales Kriterium 146
b) Rechnungstragungsgebot gem. Art. 7 Abs. 4 DSGVO 147
c) Bestimmtheit 149

d) Informiertheit der Einwilligung 150
3. Widerruf der Einwilligung 151
4. Zwischenergebnis: Einwilligung ist keine rechtssichere Grundlage 153
VI. Erforderlichkeit der Verarbeitung aufgrund berechtigter Interessen gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO 153
1. Vorliegen berechtigter Interessen 154
2. Erforderlichkeit des Trainings maschinell lernender Systeme mit personenbezogenen Daten 154
a) Pseudonymisierung als milderes, gleich geeignetes Mittel 155
aa) Relativer oder absoluter Personenbezug 155
bb) Mittel zur Identifizierung 156
cc) Rechtsfolge der Pseudonymisierung 157
b) Ergebnis: Pseudonymisierung als milderes Mittel 158
3. Kein Entgegenstehen überwiegender Interessen der betroffenen Person 159
4. Zwischenergebnis zum Training gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO 160
C. Einsatz algorithmischer Systeme im Arbeitsverhältnis 161
I. Sachlicher Anwendungsbereich von § 26 BDSG 161
1. Verarbeitung personenbezogener Daten 162
2. Zwecke des Beschäftigungsverhältnisses 162
3. Nicht automatisierte Verarbeitung auch erfasst 162
II. Persönlicher Anwendungsbereich 163
III. § 26 Abs. 2 BDSG: Einwilligung 163
1. Zentrales Merkmal: Freiwilligkeit 163
a) Freiwilligkeit im Bewerbungsstadium oder Arbeitsverhältnis 164
b) Vorteil oder gleichgelagerte Interessen i. S. d. § 26 Abs. 2 S. 2 BDSG 166
c) Folgen für die Praxis: Schwierige Beweisführung 167
d) Zwischenergebnis: Hohe Anforderungen an das Merkmal der Freiwilligkeit 168
2. Informiertheit der Einwilligung 169
3. Form 170

4. Zwischenergebnis: Einwilligung ist keine taugliche Rechtsgrundlage ... 170
IV. Art. 6 Abs. 1 lit. b DSGVO als Verarbeitungsgrundlage im Beschäftigungskontext ... 171
1. Übertragbarkeit der Grundsätze zu § 26 Abs. 1 S. 1 BDSG auf Art. 6 Abs. 1 S. 1 lit. b DSGVO? ... 171
2. Erforderlichkeit der Verarbeitung gem. § 26 Abs. 1 S. 1 BDSG und Art. 6 Abs. 1 S. 1 lit. b DSGVO ... 172
a) Kein generelles Verbot des Einsatzes algorithmischer Systeme ... 175
b) Geeignetheit ... 176
aa) Bedeutung der Qualität der Trainingsdaten ... 176
bb) Insbesondere: Wahrung des Fragerechts der Arbeitgeberin ... 177
c) Erforderlichkeit ... 178
aa) Mildere Mittel gegenüber einem algorithmischen System ... 178
bb) Gleiche Eignung ... 181
d) Angemessenheit ... 182
aa) Relevante Abwägungsgesichtspunkte ... 182
(1) Allgemeine Abwägungsgesichtspunkte ... 182
(2) Öffentlich zugängliche Daten vs. Grundsatz der Direkterhebung ... 184
(3) Interesse an objektiver Auswahlentscheidung und Bewältigung großer Datenmengen ... 185
(4) Kein Erstellen eines umfassenden Persönlichkeitsprofils ... 186
(5) Grenze: Fragerecht der Arbeitgeberin ... 187
(6) Nähe zur Menschenwürde gem. Art. 1 GRCh: Wahrung personaler Individualität ... 188
bb) Angemessenheit des Einsatzes algorithmischer Systeme ... 189
3. Zwischenergebnis zur Erforderlichkeit ... 191
V. Betriebsvereinbarungen ... 192
1. Betriebsvereinbarung als Rechtsgrundlage für die Datenverarbeitung ... 193
2. Abweichungen vom Schutzstandard der DSGVO möglich? ... 195

a) Unterschiedliche Auffassungen in Literatur und Rechtsprechung 196
aa) Keine Abweichung vom Schutzstandard der DSGVO möglich 196
bb) Abweichungen „nach unten“ nur im Ausnahmefall möglich 197
cc) Abweichung „nach oben“ möglich 198
b) Prinzipielles Schutzniveau des Art. 88 Abs. 2 DSGVO 199
c) Konsequenz: Art. 88 Abs. 1 DSGVO enthält kein „Abweichungsverbot“ 200
3. Zwischenergebnis: Betriebsvereinbarung als flexible Rechtsgrundlage 203
D. Ergebnis des Systems als Grundlage für die Auswahlentscheidung 204
I. Historie von Art. 22 DSGVO 205
1. Art. 15 DSRL als Vorgängervorschrift zu Art. 22 DSGVO 205
2. Umsetzung von Art. 15 DSRL durch Art. 6a BDSG a. F. 206
II. Rechtsnatur des Art. 22 Abs. 1 DSGVO 207
III. Telos: Schutz vor automatisierten Entscheidungen 208
1. Bezug zur Menschenwürde nach Art. 1 Abs. 1 GG 208
2. Besonders hohes Risiko durch automatisierte Entscheidungen 208
IV. Anwendungsbereich des Art. 22 Abs. 1 DSGVO bei algorithmischen Systemen in der Personalauswahl 211
1. Teleologische Reduktion des Merkmals „Entscheidung“ 211
a) Personenbezogene Bewertung 212
b) Mindestmaß an Komplexität der Entscheidung 213
2. Unterworfensein der betroffenen Person 214
3. Entscheidung beruht ausschließlich auf automatisierter Verarbeitung 214
a) Ausschließlichkeit der automatisierten Verarbeitung 214
b) Gefahr auch bei einer bloßen Entscheidungsunterstützung . 216
aa) Ankereffekt 217
bb) Overreliance 218
c) Lösung: Protokollpflicht 219
d) Zwischenergebnis zum Merkmal der Ausschließlichkeit 220
4. Rechtliche Wirkung oder erhebliche Beeinträchtigung 221
a) Auslegung der Merkmale 222

b) Positive Entscheidung auch erfasst 223
5. Ausnahmetatbestände nach Art. 22 Abs. 2 DSGVO 224
a) Entscheidung erforderlich für den Abschluss oder die Erfüllung eines Vertrags (Art. 22 Abs. 2 lit. a DSGVO) 224
aa) Maßstab der Erforderlichkeit 224
bb) Erforderlichkeit im Beschäftigungsverhältnis 225
(1) Geeignetheit 226
(2) Erforderlichkeit 226
(3) Angemessenheit 228
(4) Zwischenergebnis 229
b) Zulässigkeit aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten (Art. 22 Abs. 2 lit. b DSGVO) 229
c) Einwilligung der betroffenen Person (Art. 22 Abs. 2 lit. c DSGVO) 230
aa) Maßstab analog Art. 4 Nr. 11, 6 Abs. 1 S. 1 lit. a, 7 Abs. 4 DSGVO und § 26 Abs. 2 BDSG 230
bb) Einwilligung im Bewerbungs- und Beschäftigungsverhältnis 231
6. Schutzmaßnahmen nach Art. 22 Abs. 3 DSGVO 232
V. Ergebnis zu Art. 22 DSGVO 234
1. Art. 22 DSGVO regelmäßig nicht einschlägig 234
2. (Unsichere) Ausnahmen nach Art. 22 Abs. 2 DSGVO 235
3. Rechte nach Art. 22 Abs. 3 DSGVO 235
E. Zwischenergebnis: Rechtmäßigkeit der Datenverarbeitung 236

Kapitel 7
Weitere Pflichten der Verantwortlichen und Betroffenenrechte 241
A. DSFA gem. Art. 35 DSGVO bei algorithmischen Systemen erforderlich 241
I. Datenschutzfolgenabschätzung als Instrument für Transparenz .. 243
II. Durchführung der DSFA 244
1. Verarbeitungsverzeichnis gem. Art. 30 DSGVO 244
2. Mindestinhalt der DSFA 245
3. Risikobewertung und geplante Maßnahmen zur Risikominimierung 245
4. Konsultationspflicht der Aufsichtsbehörde 246

B. Informationspflichten gem. Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO ... 246
I. Nur ausschließlich automatisierte Entscheidungen erfasst ... 248
II. Zeitpunkt der Informationspflichten nicht maßgeblich für den Inhalt ... 249
III. Inhalt der Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO 250
1. Aussagekräftige Informationen über die involvierte Logik ... 250
a) Involvierte Logik ... 250
b) Aussagekräftige Informationen ... 252
2. Tragweite und Auswirkungen der Verarbeitung ... 253
IV. Umsetzung der Informationspflichten in der Praxis ... 253
1. Ausgangsproblem: Schriftliche Erklärungen und Komplexität 253
2. Allgemeine Vorgaben des Art. 12 Abs. 1 DSGVO ... 254
a) Präzise und transparente Form ... 254
b) Verständlichkeit und leichte Zugänglichkeit ... 255
3. Transparenz durch visuell wahrnehmbare Informationen ... 256
a) Bildsymbole ... 256
b) Ablaufdiagramme ... 256
c) Gamification ... 257
V. Informations-/Erklärungspflichten *de lege ferenda* ... 257
1. Informationspflichten auch bei teilautomatisierten Entscheidungen ... 257
2. Pflicht zur Verwendung visueller Techniken ... 258
3. Recht auf Begründung der Entscheidung als Lösung? ... 259
C. Rechte der betroffenen Person ... 261
I. Auskunftsrecht gem. Art. 15 DSGVO ... 261
1. Zweistufiges Auskunftsrecht ... 261
2. Umfang des Auskunftsrechts: Auskunft über die Output-Daten ... 262
II. Recht auf Berichtigung gem. Art. 16 DSGVO ... 264
III. Recht auf Löschung gem. Art. 17 DSGVO ... 266
1. Daten sind für Erhebungs- und Verarbeitungszwecke nicht mehr erforderlich (Art. 17 Abs. 1 lit. a DSGVO) ... 267
2. Betroffene Person widerruft ihre Einwilligung (Art. 17 Abs. 1 lit. b DSGVO) ... 268

D. Zwischenergebnis: Erweiterung der Informationspflichten *de lege ferenda* 268

Teil 2
Zusammenfassung *273*

Teil 3
Anforderungen nach dem AGG *279*

Kapitel 8
Benachteiligung durch algorithmische Systeme *281*
A. Mögliche Benachteiligungen 281
I. Bewerbungssystem filtert bestimmte Gruppen heraus 281
II. Negativbeispiel *COMPAS* 282
III. Arbeitsmarkt-Chancen-Modell aus Österreich 284
1. Funktionsweise des AMAS 284
2. Untersagung von der Datenschutzbehörde 285
3. Kassation des Verbots durch das BVwG Österreich 287
B. Gründe für eine Benachteiligung durch Algorithmen 288
I. Mangelnde Qualität der Trainingsdaten 288
II. Berücksichtigung von *Proxy*-Variablen 289
III. Vorurteile der Entwicklerinnen und Wahl der Parameter 290
C. Zwischenergebnis: Benachteiligungen als Alltagsphänomen 291

Kapitel 9
Schutzrahmen des AGG *293*
A. Verstoß gegen das Benachteiligungsverbot 293
I. Anwendungsbereich des AGG 293
1. Anwendungsbereich eröffnet beim Bezug zum Arbeitsverhältnis 293
2. Anwendungsbereich eröffnet bei der Sammlung von Trainingsdaten 294
II. Verstoß gegen das Benachteiligungsverbot 296
1. Unmittelbare Benachteiligung 296
a) Behandlung durch ein algorithmisches System 296

b) Erweiterung des Anwendungsbereichs des § 1 AGG de lege ferenda ... 298
c) Kausalität ... 300
2. Mittelbare Benachteiligung ... 301
III. Rechtfertigung ... 302
1. Rechtfertigung einer unmittelbaren Benachteiligung ... 302
a) Gem. §§ 8-10 AGG ... 302
b) Gem. § 5 AGG ... 303
2. Rechtfertigung einer mittelbaren Benachteiligung ... 303
a) Rechtmäßiges Ziel ... 304
b) Verhältnismäßigkeit ... 304
aa) Geeignetheit ... 304
bb) Erforderlichkeit ... 306
cc) Angemessenheit ... 307
dd) Zwischenergebnis ... 309
B. Haftung bei Verstößen gegen das Benachteiligungsverbot ... 310
I. Schadensersatz nach § 15 Abs. 1 S. 1 AGG ... 310
1. Vertretenmüssen der Arbeitgeberin ... 310
a) Eigenes Verschulden der Arbeitgeberin – Grundsätze der Wissenszurechnung ... 311
b) Zurechnung des Verschuldens der Herstellerin gem. § 278 S. 1 BGB ... 314
2. § 278 S. 1 BGB analog bei algorithmischen Systemen ... 316
3. Geringer Anwendungsbereich des § 15 Abs. 1 S. 1 AGG ... 318
II. Entschädigung nach § 15 Abs. 2 S. 1 AGG ... 318
1. Beweiserleichterung nach § 22 AGG bei algorithmischen Systemen ... 318
a) Blackbox-Auswertungen als Indiz ... 319
b) Indizien aufgrund der Informationspflichten nach Art. 12 ff. DSGVO ... 320
c) Zwei-Stufen-Modell der Darlegungslast nach Grünberger ... 321
2. Fazit: gerechte Lösung durch Zwei-Stufen-Modell der Darlegungslast ... 324
C. Zwischenergebnis zum Schutzrahmen des AGG ... 325

Teil 3
Zusammenfassung *333*

Teil 4
Anforderungen aufgrund einer zukünftigen KI-VO *339*

Kapitel 10
Vorgaben für Hochrisiko-KI-Systeme *341*
A. Akteurinnen einer zukünftigen KI-VO 341
B. Überblick über die Anforderungen nach Kapitel 2 KI-VO-KOM 343
I. Vorgaben für die Trainingsdatenqualität gem. Art. 10 Abs. 3, 4 KI-VO-KOM 345
1. Auslegung der Merkmale des Art. 10 Abs. 3 KI-VO-KOM 346
a) Relevanz 347
b) Repräsentativität 348
c) Fehlerfreiheit 349
d) Vollständigkeit 350
e) Geeignete statistische Merkmale 351
2. Handhabbare Umsetzung in der Praxis durch Art. 10 Abs. 3 KI-VO-PARL 352
II. Transparenz i. S. d. Art. 13 KI-VO-KOM und KI-VO-PARL 355
1. Vorgaben des Art. 13 KI-VO-KOM 355
2. Definition von Transparenz in Art. 13 Abs. 1 KI-VO-PARL 356
C. Ausgestaltung der Vorschriften und Rechtsfolgen bei Nichteinhaltung 357
D. Zwischenergebnis zu den Vorgaben der Hochrisiko-KI-Systeme 359

Kapitel 11
KI-VO-KOM und DSGVO: Widerspruch oder (sinnvolle) Ergänzung? *363*
A. Zusammenspiel verschiedener Risikobewertungen und DSFA 363
I. Art. 9 KI-VO-KOM 363
II. Art. 29a KI-VO-PARL und Art. 35 DSGVO 368
III. Art. 54 Abs. 1 lit. c KI-VO-PARL und Art. 35 DSGVO 370
IV. Zwischenergebnis: Gleichlauf der Pflichten nach einer zukünftigen KI-VO und der DSGVO nicht immer sinnvoll 370
B. (K)eine Überschneidung mit Art. 9 DSGVO? 371

I. Regelungsgehalt von Art. 10 Abs. 5 KI-VO-KOM ... 372
II. Ausnahme nach Art. 9 Abs. 2 lit. g DSGVO ... 375
III. Eigenständige Rechtsgrundlage? ... 376
IV. Ausweitung des Anwendungsbereichs des Art. 10 Abs. 5 KI-VO-KOM ... 378
V. Zwischenergebnis: Keine Überschneidung mit Art. 9 DSGVO ... 379
C. Hohe Datenqualität vs. Grundsatz der Datenminimierung ... 380
D. Menschliche Überwachung von Hochrisiko-KI-Systemen ... 382
I. Kritik an Art. 14 Abs. 1 KI-VO-KOM ... 382
II. Art. 14 KI-VO-PARL als praxistauglichere Vorschrift? ... 383
E. Art. 54 KI-VO-KOM vs. Art. 6 Abs. 4 DSGVO ... 384
F. Betroffenenrechte nach der DSGVO vs. Recht auf Erklärung ... 386
G. Zwischenergebnis: Vorschriften des KI-VO-KOM berücksichtigen die DSGVO nicht hinreichend ... 389

Teil 4
Zusammenfassung ... 393

Kapitel 12
Zusammenfassung der Ergebnisse ... 399
A. Algorithmische Systeme: technischer Hintergrund und Einsatz ... 399
B. Transparenzanforderungen an algorithmische Systeme ... 401
C. Erfordernis einer Verarbeitungsgrundlage ... 404
D. Verbot ausschließlich automatisierter Entscheidungen ... 410
E. Anforderungen nach dem AGG ... 412
F. Anforderungen nach einer zukünftigen KI-VO ... 418
Literaturverzeichnis ... 427

Abkürzungsverzeichnis

AC	Amicus Curiae
AcP	Archiv für die civilistische Praxis
Adv. Sc.	Advanced Science
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGG	Allgemeines Gleichbehandlungsgesetz
AMAS	Arbeitsmarkt-Chancen-Assistenzsystem
AMS	Österreichischer Arbeitsmarktservice
AöR	Archiv des öffentlichen Rechts
ArbRAktuell	Arbeitsrecht Aktuell
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl. I	Bundesgesetzblatt Teil I
BMAS	Bundesministerium für Arbeit und Soziales
Brook. L. Rev.	Brooklyn Law Review
BT-Drs.	Drucksachen des Deutschen Bundestages
BVerfG	Bundesverfassungsgericht
BVMed	Bundesverband Medizintechnologie
Cal. L. Rev.	California Law Review
CMLR	Common Market Law Review
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
CR	Computer und Recht
Dako	Datenschutz konkret
DB	Der Betrieb

DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DSRITB	Deutsche Stiftung für Recht und Informatik
DSRL	Richtlinie 95/94/EG
DuD	Datenschutz und Datensicherheit
EALR	ELSA Austria Law Review
EDSA	Der Europäische Datenschutzausschuss
EGMR	Europäischer Gerichtshof für Menschenrechte
EGMR-E	EGMR-Entscheidungssammlung
EMRK	Europäische Menschenrechtskonvention
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
EuZ	Zeitschrift für Europarecht
EuZA	Europäische Zeitschrift für Arbeitsrecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
FQS	Forum Qualitative Sozialforschung
GbR	Gesellschaft bürgerlichen Rechts
GG	Grundgesetz
GPR	Zeitschrift für das Privatrecht der Europäischen Union
GRCh	Charta der Grundrechte der Europäischen Union
HBDI	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HmbBfDI	Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
IJACSA	International Journal of Advanced Computer Science and Applications
IJSEA	International Journal of Software Engineering and Its Applications
Int J Law Info Tech	International Journal of Law and Information Technology
IPRax	Praxis des Internationalen Privat- und Verfahrensrechts

IR	InfrastrukturRecht
ITRB	IT-Rechtsberater
JI-Richtlinie	Richtlinie (EU) des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
JURA	JURA
JuS	Juristische Schulung
JW	Juristische Wochenschrift
JZ	Juristenzeitung
K&R	Kommunikation und Recht
KI	Künstliche Intelligenz
KIA	KI-Agenten
KI-HaftRL-E	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM(2022) 496 final 2022/0303(COD)
KI-VO	KI-Verordnung
KI-VO-KOM	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM (2021) 206 final
KI-VO-PARL	Gesetz über künstliche Intelligenz, Abänderungen, die das Europäische Parlament am 14. Juni 2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union

	(COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)), P9_TA(2023)0236
KI-VO-RAT	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, Allgemeine Ausrichtung, 14954/22
KZfSS	Kölner Zeitschrift für Soziologie und Sozialpsychologie
LAG	Landesarbeitsgericht
LRP	Layer-Wise Relevance Propagation
LTZ	Legal Tech Zeitschrift
MMR	Multimedia und Recht
MMR-Aktuell	Multimedia und Recht Aktuell
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenzeitung
NJW-RR	NJW-Rechtsprechungs-Report
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZA-Beil.	NZA-Beilage
NZA-RR	NZA-Rechtsprechungs-Report Arbeitsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
öAT	Zeitschrift für das öffentliche Arbeits- und Tarifrecht
Österreich Z Soziol	Österreichische Zeitschrift für Soziologie
PPVk	Positive Predictive Value
RdA	Recht der Arbeit
RDi	Recht Digital
RDV	Recht der Datenverarbeitung
ROC AUC	Receiver-Operator Characteristic Area under the curve
RW	Rechtswissenschaft
S. Cal. L. Rev.	Southern California Law Review
SAE	Sammlung arbeitsrechtlicher Entscheidungen
SLU	Saint Louis University Law Journal
SSRN Journal	Social Science Research Network Journal

TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UCLA Law Rev.	UCLA Law Review
Univ. Pa. Law Rev.	University of Pennsylvania Law Review
VuR	Verbraucher und Recht
XAI	eXplainable AI
ZD	Zeitschrift für Datenschutz
ZD-Aktuell	Zeitschrift für Datenschutz Aktuell
ZdiW	Zeitschrift für das Recht der digitalen Wirtschaft
ZESAR	Zeitschrift für europäisches Sozial- und Arbeitsrecht
ZfA	Zeitschrift für Arbeitsrecht
ZfDR	Zeitschrift für Digitalisierung und Recht
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZGE	Zeitschrift für geistiges Eigentum
ZIIR	Zeitschrift für Informationsrecht
ZIP	Zeitschrift für Wirtschaftsrecht und Insolvenzpraxis
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik

Einleitung*

„The rise of powerful artificial intelligence will be either the best, or the worst thing, ever to happen to humanity."[1]

Diese Aussage traf Stephen Hawking im Jahr 2016. Auch heute ruft künstliche Intelligenz (KI, englisch *artificial intelligence*) bei vielen Menschen Unbehagen hervor. Schnell wird der Bezug zu dystopischen Filmen hergestellt, in denen mithilfe von KI erschaffene menschenähnliche Wesen ein eigenes Bewusstsein entwickeln.[2] Ist von KI die Rede, sind damit meist Methoden des maschinellen Lernens gemeint. [3] Mit solchen Lernmethoden werden maschinell lernende Systeme (häufig auch als KI-System bezeichnet) trainiert, die auf neue (unbekannte) Daten angewendet werden können.[4] Kommt ein System nicht unter Einsatz maschineller Lernmethoden zustande, handelt es sich um ein nicht-lernendes System.[5] Sowohl maschinell lernende als auch nicht-lernende Systeme lassen sich unter dem Begriff algorithmische Systeme zusammenfassen.

Auch wenn Szenarien, wie in etwaigen dystopischen Filmen gezeigt, bloße Fiktion sind, werden solche algorithmischen Systeme längst eingesetzt. In vielen Bereichen nehmen wir sie kaum noch bewusst wahr: *Netflix* empfiehlt einen Film auf Grundlage der bereits angeschauten Filme. Assistenzprogramme wie *Siri* oder *Alexa* können das gesprochene Wort verstehen und einfache Anweisungen umsetzen, wie etwa Termine in den

---

* Aus Gründen der besseren Lesbarkeit wird in der Arbeit das generische Femininum verwendet. Die Formulierungen umfassen Personen aller Geschlechter gleichermaßen.

[1] Rede von Stephen Hawking bei der Eröffnung des *Leverhulme Centre for the Future of Intelligence* am 19.10.2016, Minute 4:25, https://perma.cc/5SFD-67D7 (archiviert am 04.03.2023).

[2] S. etwa der Film „Ex Machina", zum Inhalt s . überblicksartig den Wikipedia-Artikel, https://perma.cc/RG2G-9Q72 (archiviert am 06.01.2023).

[3] S. Kapitel 1 C. (S. 12).

[4] Kapitel 1 A. (S. 9).

[5] Kapitel 1 A. (S. 9).

Kalender einzutragen oder das Licht anzuschalten. Das Smartphone wird per Gesichtserkennung entsperrt. Erst Ende des Jahres 2022 veröffentlichte *OpenAI* das Sprachprogramm *ChatGPT*, das auch komplexe Aufgaben – wie etwa das Verfassen eines Gedichts zu einem bestimmten Thema – umsetzen kann. Die Software erweckt fast den Eindruck, man kommuniziere mit einem Menschen. Solche Programme werden in Zukunft nicht nur das Prüfungswesen an den Hochschulen vor neue Herausforderungen stellen.[6] Vielmehr besteht auch die Gefahr, dass Falschinformationen durch derartige Programme verbreitet werden. Der US-Professor Carl T. Bergstrom warnt davor, dass Modelle wie *ChatGPT* „darauf trainiert [sind], Dinge zu erfinden, die völlig plausibel klingen"[7].

Mit Blick auf zahlreiche Anwendungsfelder ist es nicht verwunderlich, dass algorithmische Systeme auch bereits bei arbeitsrechtlichen Auswahlentscheidungen eingesetzt werden. Sie sollen insbesondere dabei helfen, in kürzerer Zeit objektive Entscheidungen zu treffen. Die Möglichkeiten sind vielfältig: Anstelle eines herkömmlichen Lebenslaufs und eines Anschreibens kann man etwa ein Video von sich aufnehmen, das anschließend von einem algorithmischen System hinsichtlich bestimmter Persönlichkeitsmerkmale analysiert wird. Oder aber man kommuniziert bei Fragen zur Bewerbung mit einem Chatbot.

Auf rechtlicher Ebene werfen algorithmische Systeme eine Vielzahl an Fragestellungen auf: Welche Voraussetzungen müssen sie erfüllen, damit sie rechtssicher eingesetzt werden können? Welche Schwierigkeiten bringt die Verarbeitung personenbezogener Daten durch derartige Systeme mit sich? Welche Besonderheiten sind im Bewerbungs- und Arbeitsverhältnis zu berücksichtigen?

---

[6] *Bach/Weßels*, Das Ende der Hausarbeit, FAZ, 21.12.2022, https://perma.cc/HD9C-KSGK (archiviert am 04.02.2023).

[7] *Kühl*, Gut erfunden ist halb geglaubt, Zeit Online 06.12.2022, https://perma.cc/Y86E-YRCU (archiviert am 04.03.2023).

Algorithmische Systeme sind längst Gegenstand juristischer Diskussion.[8] Sowohl auf unionaler als auch auf nationaler Ebene gibt es zahlreiche Vorschriften, die beim Training und beim Einsatz algorithmischer Systeme relevant werden können. Neben der im Jahr 2018 in Kraft getretenen DSGVO[9] gibt es Entwürfe der Komission[10] (KI-VO-KOM), des Rats[11] (KI-VO-RAT) und des Parlaments[12] (KI-VO-PARL) für eine KI-Verordnung. Seit Mitte 2022 gilt der Data-Governance Act[13]. Außerdem sind seit Ende 2022 der Digital Services Act[14] sowie der Digital Markets Act[15] in Kraft.

---

[8] *Krause*, Digitalisierung der Arbeitswelt - Herausforderungen und Regelungsbedarf, 2016, B 11 ff.; *Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz* (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022; *Dederer/Shin* (Hrsg.), Künstliche Intelligenz und juristische Herausforderungen, 2021; *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023; *Knitter*, Digitale Weisungen, 2022.

[9] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), L 119/1.

[10] Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM (2021) 206 final.

[11] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, Allgemeine Ausrichtung, 14954/22.

[12] Gesetz über künstliche Intelligenz, Abänderungen, die das Europäische Parlament am 14. Juni 2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)), P9_TA(2023)0236.

[13] Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz), COM(2020) 767 final.

[14] Verordnung des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), L 277/1.

[15] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), L 265/1; s. dazu auch den Podcast von Philipp Hacker zum Thema „Is the DMA the real AI regulation", https://perma.cc/GXV7-JPN9 (archiviert am 11.02.2023).

Zudem wurde Ende 2022 ein Vorschlag für eine KI-Haftungsrichtlinie (KI-HaftRL-E) vorgelegt.[16] Hinsichtlich des Data Acts[17] hat sich das Europäische Parlament mit dem Rat der EU am 28. Juni 2023 geeinigt. Das Parlament hat den Data Act am 09. November 2023 mit 481 zu 31 Stimmen bei 71 Enthaltungen angenommen.[18] Der Data Act wird am zwanzigsten Tag seiner Veröffentlichung im Amtsblatt in Kraft treten und zwanzig Monate später anwendbar sein.[19]

Auf nationaler Ebene regelt das BDSG die Verarbeitung personenbezogener Daten. Außerdem können sich auch diskriminierungsrechtliche Fragen stellen, wenn algorithmische Systeme eingesetzt werden. An dieser Stelle rückt das Allgemeine Gleichbehandlungsgesetz in den Fokus.

Ziel dieser Arbeit ist es, arbeitsrechtliche Auswahlentscheidungen mittels algorithmischer Systeme unter drei rechtlichen Gesichtspunkten zu beleuchten: aus datenschutzrechtlicher und antidiskriminierungsrechtlicher Sicht sowie aus Sicht des KI-VO-KOM, des KI-VO-RAT und des KI-VO-PARL. Schwerpunkt liegt dabei auf den datenschutzrechtlichen Fragenstellungen beim Training und Einsatz algorithmischer Systeme. Um den Umfang der Arbeit sinnvoll zu begrenzen, werden indes nicht alle der oben genannten Rechtsquellen untersucht, die für algorithmische Systeme grundsätzlich relevant sein können. Außer Betracht bleiben insbesondere der Data Act, der Data Governance Act, der Digital Services Act und der Digital Markets Act.

---

[16] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM(2022)496 final.

[17] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM(2022) 68 final; hierzu *Bomhard/Merkle*, RDi 2022, 168.

[18] https://perma.cc/52HU-J8GF (archiviert am 12.11.2023).

[19] Art. 42 Abs. 1 und 2 Data Act, zur Presseerklärung s. https://perma.cc/UR5F-E7PG (archiviert am 30.06.2023).

Gang der Untersuchung

Die Arbeit gliedert sich in vier Teile. Im ersten Teil der Arbeit wird zunächst eine Begriffsbestimmung vorgenommen [1]: Was ist unter algorithmischen Systemen zu verstehen? Nachdem die technischen Grundlagen erläutert wurden [2], werden Anwendungsszenarien derartiger Systeme im Überblick vorgestellt [3]. Sodann werden menschliche und algorithmische Entscheidungen miteinander verglichen.[4] Schließlich wird der Begriff der Transparenz im Kontext algorithmischer Entscheidungen untersucht.[5] Welche Anforderungen man an die Transparenz algorithmischer Entscheidungen stellt, ist für die folgende Untersuchung an vielen Stellen relevant.[6]

Der zweite Teil, der gleichzeitig auch den Schwerpunkt der Arbeit bildet, setzt sich mit den Anforderungen an algorithmische Systeme nach der DSGVO und dem BDSG auseinander. Dabei wird zwischen drei Verarbeitungsstadien unterschieden: Zunächst werden die datenschutzrechtlichen Fragen untersucht, die sich beim Training algorithmischer Systeme stellen.[7] Beim zweiten Verarbeitungsstadium geht es um den konkreten Einsatz algorithmischer Systeme.[8] Im letzten Verarbeitungsstadium geht es darum, dass das vom algorithmischen System generierte Ergebnis die Grundlage für die (menschliche) Entscheidung bildet. In diesem Stadium liegt der Fokus auf Art. 22 DSGVO.[9]

---

[1] Kapitel 1 A. (S. 9).
[2] Kapitel 1 B. (S. 10); Kapitel 1 C. (S. 12).
[3] Kapitel 2 (S. 23).
[4] Kapitel 3 (S. 33).
[5] Kapitel 4 (S. 39).
[6] Kapitel 7 B.IV. (S. 253); Kapitel 9 B.II.1. (S. 318); Kapitel 10 B.II. (S. 355).
[7] Kapitel 6 B. (S. 117).
[8] Kapitel 6 C. (S. 161).
[9] Kapitel 6 D. (S. 204).

Der dritte Teil der Arbeit setzt sich mit dem AGG auseinander. Beleuchtet wird, wie Benachteiligungen durch algorithmische Systeme zustande kommen.[10] Anschließend wird erläutert, wann ein Verstoß gegen ein Benachteiligungsverbot vorliegt[11] und unter welchen Bedingungen man bei Verstößen gegen das Benachteiligungsverbot haftet[12].

Der letzte Teil beschäftigt sich mit dem KI-VO-KOM, dem KI-VO-RAT sowie dem KI-VO-PARL. Anfangs werden die Vorgaben für Hochrisiko-KI-Systeme erläutert.[13] Im nächsten Abschnitt werden einige für den Untersuchungsgegenstand relevante Vorgaben der Entwürfe mit den Vorgaben der DSGVO verglichen.[14] Stehen die Vorschriften des KI-VO-KOM, KI-VO-RAT und KI-VO-PARL im Widerspruch zu den Vorschriften der DSGVO oder bilden sie eine sinnvolle Ergänzung? Zu dem Verhältnis zwischen zukünftiger KI-VO und DSGVO wird sodann ein Fazit[15] gezogen, bevor die wesentlichen Ergebnisse der Arbeit zusammengefasst werden.[16]

---

[10] Kapitel 8 (S. 281).
[11] Kapitel 9 A. (S. 293).
[12] Kapitel 9 B. (S. 310).
[13] Kapitel 10 (S.341).
[14] Kapitel 11 (S. 363).
[15] Kapitel 11 G. (S. 389).
[16] Kapitel 12 (S. 399).

Teil 1

Algorithmische Systeme im Kontext arbeitsrechtlicher Auswahlentscheidungen

KI, algorithmische Systeme, maschinelles Lernen, neuronale Netze, *Deep Learning*, *Big Data*: Diese Begriffe sind in der rechtswissenschaftlichen Forschung und Diskussion mittlerweile allgegenwärtig.[1] Insbesondere beim Begriff KI fehlt bislang eine einheitliche Definition.[2] Für die rechtliche Analyse der aufgeführten Anwendungsszenarien[3] ist eine Begriffsbestimmung sowie eine technische Einführung eine notwendige Voraussetzung. Diese Arbeit ist eine rechtswissenschaftliche Dissertation und vermag es deshalb nicht, sich mit allen mathematischen und technischen Einzelheiten zu beschäftigen. Zunächst wird daher eine Begriffsbestimmung vorgenommen[4], gefolgt von einer technischen Einführung[5], die sachlich notwendig ist und die eine Rechtswissenschaftlerin ohne Vorkenntnisse verstehen sollte. Deshalb wird auch bewusst auf Formeln verzichtet.

Nachdem die Anwendungsszenarien vorgestellt wurden, werden wesentliche Unterschiede zwischen menschlichen und algorithmischen Entscheidungen beleuchtet[6]. Schließlich wird näher auf den Aspekt der Transparenz[7] eingegangen, der insbesondere bei maschinell lernenden Entscheidungssystemen eine entscheidende Rolle einnimmt.[8] Auch für die spätere rechtliche Beurteilung ist es notwendig herauszuarbeiten, was die Arbeit allgemein unter dem Begriff Transparenz versteht und aus welchen Bestandteilen dieser sich zusammensetzt.

---

[1] S. etwa: *Dzida*, NZA 2017, 541; *Geminn*, ZD 2021, 354; *Hoffmann-Riem*, AöR 142 (2017), 1; *Malorny*, JuS 2022, 289; *Söbbing*, MMR 2021, 111; *Strecker*, RDi 2021, 124.

[2] *Geminn*, ZD 2021, 354; *Rüfner*, in: Dederer/Shin (Hrsg.), Künstliche Intelligenz und juristische Herausforderungen, 2021, S. 15, 17; auch im Betriebsverfassungsrecht wird der Begriff zwar verwendet, aber nicht näher definiert: *Frank/Heine*, NZA 2021, 1448; zur Definition von KI in einer zukünftigen KI-VO s. Kapitel 5 A.IV.3.a) (S. 77).

[3] Kapitel 2 (S. 23).

[4] Kapitel 1 A. (S. 9).

[5] Kapitel 1 B. (S. 10).

[6] Kapitel 3 (S. 33).

[7] Kapitel 4 (S. 39).

[8] Statt vieler: *Janal*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 123, 123 ff.

Kapitel 1

Begriffsbestimmung und technische Grundlagen

A. Algorithmische Systeme

Unter dem Begriff „algorithmisches System“ versteht diese Arbeit ein Softwaresystem, das Menschen bewertet und algorithmenbasiert Entscheidungen trifft.[1] Von einem *System* ist deshalb die Rede, weil es aus mindestens zwei Algorithmen besteht[2]: Der erste Algorithmus lernt aus Daten etwa, wie Personen in der Vergangenheit kategorisiert wurden.[3] Beispielsweise kann es sein, dass Personen, die immer pünktlich zur Arbeit kommen, besonders verlässlich sind und daher entsprechend kategorisiert werden können. Daraus ergibt sich ein Regelwerk, in das neue Daten von unbekannten Personen eingepflegt werden können. Sodann berechnet der zweite Algorithmus etwa die Kategorie, in die die Person einzuordnen ist.[4] Während der erste Algorithmus komplexer ist und meist unter Einsatz maschinellen Lernens zustande gekommen ist, ist der zweite Algorithmus weniger komplex und liefert das auf Basis des *Inputs* passende Ergebnis.[5] Häufig werden solche Systeme unterstützend eingesetzt, etwa um eine Vorauswahl an Bewerberinnen zu treffen.[6] Sie werden daher auch

---

[1] *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018, S. 13; s. dazu auch: *Müller/Kirchner/Schüßler*, in: Kuschel/Asmussen/Golla (Hrsg.), Intelligente Systeme – intelligentes Recht, 2021, S. 85, 87.

[2] *Gärtner*, Smart HRM, 2020, S. 18; *Prietl*, feministische studien 2019, 303, 306.

[3] *Zweig*, Wo Maschinen irren können, 2018, S. 13.

[4] *Dies.*, Wo Maschinen irren können, 2018, S. 13.

[5] *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 10; *Zweig*, Wo Maschinen irren können, 2018, S. 11.

[6] Kapitel 2 A (S. 24).

„Entscheidungsunterstützungssysteme“ (engl. *decision support systems*) genannt.[7]

Enthalten algorithmische Systeme aber keine Lernalgorithmen[8], sondern nur klassische Algorithmen[9], die rein regelbasiert zu einer bestimmten Entscheidung kommen, fallen solche Systeme zwar auch unter die Definition eines algorithmischen Systems. Sie basieren aber nicht auf Methoden des maschinellen Lernens. Der Begriff „maschinell lernendes System“ wird im Folgenden daher nur für derartige algorithmische Systeme verwendet, die mithilfe maschineller Lernmethode zustande gekommen sind. Mit dem Begriff „KI-System“ sind ebenfalls maschinelle lernende Systeme gemeint. Der Begriff des KI-Systems bzw. Hochrisiko-KI-Systems wird vor allem im Kontext einer zukünftigen KI-VO verwendet, weil in den drei Verordnungsentwürfen dieser Begriff gewählt wird.[10] Im Übrigen handelt es sich um nicht-lernende Systeme.[11]

B. Klassische Algorithmen und Lernalgorithmen

Algorithmische Systeme enthalten in der Regel sowohl klassische als auch lernende Algorithmen: Ein klassischer Algorithmus ist eine eindeutige Handlungsvorschrift zur Lösung eines (mathematischen) Problems.[12] Auch ein Rezept für ein bestimmtes Gericht ist z. B. ein Algorithmus: Die Zutaten und die einzelnen Schritte (*Inputs*) sind exakt aufgelistet und sollen

---

[7] *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 14; vgl. *Kumar*, Journal of Artificial Intelligence and Capsule Networks 2020, 185; *Zweig*, Wo Maschinen irren können, 2018, S. 12.

[8] S. dazu sogleich unter: Kapitel 1 B. (S. 10).

[9] S. dazu sogleich unter: Kapitel 1 B. (S. 10).

[10] Kapitel 5 A.IV.3.a) (S. 77).

[11] S. dazu: *Kalogeropoulos/Lammers/Brehm-Müller u.a.,* 1, 6, https://perma.cc/UH3M-Q66D (archiviert am 07.11.2023).

[12] *Berberich*, in: Kerstin/Lampert/Rothkopf (Hrsg.), Wie Maschinen lernen, 2019, S. 11; *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 9; *Martini*, Blackbox Algorithmus, 2018, S. 17.

nacheinander durchgeführt werden. Am Ende steht ein zum Verzehr bereites Gericht (*Output*) auf dem Tisch.

Im Folgenden sind mit Algorithmen *Computer*algorithmen gemeint. Sie beschreiben Probleme mathematisch exakt und sind durch eine Programmiersprache repräsentiert.[13] Ein Problem könnte z. B. sein, die kürzeste Fahrtstrecke (*Output*) von einem Startpunkt zum Ziel zu berechnen. Als *Input* können verschiedene Daten wie das zur Verfügung stehende Fahrzeug, Straßenkarte oder Ziel und Ausgangspunkt der Fahrerin dienen. Wie man vom *Input* auf den gewünschten *Output* kommt, beschreibt der Algorithmus.[14] Setzt sich ein algorithmisches System aus derartigen Algorithmen zusammen, kommt es rein regelbasiert zu dem jeweiligen Ergebnis und funktioniert nach dem „Wenn-Dann-Prinzip“:[15] Wenn bestimmte Voraussetzungen erfüllt sind, dann kommt der Algorithmus zu einem bestimmten Ergebnis.

Lernalgorithmen unterscheiden sich von klassischen Algorithmen insofern, dass ihnen nicht genau vorgegeben wird, *wie* sie ein Problem lösen, sondern wie sie aus ihrer Erfahrung lernen können, ein Problem *besser* zu lösen.[16] Lernende Algorithmen können Muster in Datenmengen erkennen, daraus Rückschlüsse ziehen und ihr „Verhalten“ entsprechend anpassen.[17] Wie das funktioniert, wird erklärt, wenn die einzelnen Lernstile vorgestellt werden.[18]

---

[13] Vgl. *Hoffmann-Riem*, AöR 142 (2017), 1, 3; *Martini*, Blackbox Algorithmus, 2018, S. 18; *Zweig*, Wo Maschinen irren können, 2018, S. 11.

[14] *Ernst*, JZ 2017, 1026, 1026 f.; *Zweig*, Wo Maschinen irren können, 2018, S. 11; ein bekannter Algorithmus zur Lösung des „kürzesten-Weg-Problems“ ist der Dijkstra Algorithmus s. *Panitanarak*, in: Berry/Mohamed/Yap (Hrsg.), Supervised and Unsupervised Learning for Data Science, 2020, 39.

[15] *Hoppe*, in: Hartmann (Hrsg.), KI & Recht kompakt, 2020, S. 1, 7; *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 12.

[16] *Berberich*, in: Kerstin/Lampert/Rothkopf (Hrsg.), Wie Maschinen lernen, 2019, S. 11, 19; *Zweig*, Wo Maschinen irren können, 2018, S. 12.

[17] *Martini*, Blackbox Algorithmus, 2018, S. 19 f.; *Hoffmann-Riem*, in: Unger/Ungern-Sternberg (Hrsg.), Demokratie und künstliche Intelligenz, 2019, 134; *Nink*, Justiz und Algorithmen, 2021, S. 204.

[18] S. Kapitel 1 C.I. (S. 15).

Lernalgorithmen werden beim sog. maschinellen Lernen eingesetzt[19], welches wiederum ein Teilgebiet von KI ist.[20]

C. Maschinelles Lernen als Teilgebiet von KI

KI „is the study of how to make computers do things at which, at the moment, people are better"[21]. Diese von *Elaine Rich* stammende Definition bringt auf den Punkt, was KI-Forschung ausmacht: Neue Technologien und Algorithmen bilden kognitive Fähigkeiten des Menschen nach, um bestimmte Aufgaben zu bewältigen.[22]

Unterschieden wird in (juristischer) Literatur häufig zwischen „starker" und „schwacher" KI.[23] Die schwache KI übernimmt nur eine bestimmte und sehr eingegrenzte Aufgabe.[24] Sie kann z. B. zur Bilderkennung eingesetzt werden: Handelt es sich bei dem Bild um einen Chihuahua oder einen Muffin? [25] Welche Zahl verbirgt sich hinter der handgeschriebenen Ziffer? Das maschinell lernende System ist in der Lage, eine Lösung zu einem Problem zu finden, ohne dabei zu wissen, was das Problem eigentlich ist.[26] Es kennt die

---

[19] *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen, 2018, S. 8.

[20] S. *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 3; in Expertenkreisen gilt maschinelles Lernen als „Schlüsseltechnologie" von KI, s. *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen, 2018, S. 8.

[21] *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 3; *Rich*, Computers and the Humanities 1985, 117.

[22] S. *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 285; *Hartmann* (Hrsg.), KI & Recht kompakt, 2020, V, Vorwort.

[23] Taeger/Pohle ComputerR-HdB/*Deusch/Eggendorfer*, Teil 5. 50.1. II. 5. a) Rn. 232 m ff.; *Gärtner*, Smart HRM, 2020, S. 21; *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 2.; *Bittner/Debowski/Lorenz u.a.*, NZV 2021, 505; *Bleckat*, DuD 2020, 194.

[24] Vgl. *Braegelmann/Kaulartz*, in: Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 4.

[25] *Togootogtokh/Amartuvshin*, Deep Learning Approach for Very Similar Objects Recognition Application on Chihuhua and Muffin Problem, https://perma.cc/SGH3-XGEU (archiviert am 07.11.2023).

[26] Vgl. *Gärtner*, Smart HRM, 2020, S. 21; *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 15.

Zusammenhänge zwischen einzelnen Parametern, kann aber die einzelnen Bestandteile und Ergebnisse nicht erklären oder in Beziehung zu einer übergeordneten Instanz, wie etwa Wissen über bestimmte Regeln, setzen.[27] Das ist für Menschen mühelos möglich.[28]

Die starke KI hingegen zielt auf eine Imitation des Menschen ab.[29] Sie soll ein Bewusstsein wie ein Mensch entwickeln. Bisherige Ansätze fallen alle unter die schwache KI. [30] Bisherige maschinell lernende Systeme sind auf Anwendungsprobleme ausgerichtet, nicht aber darauf, Probleme kontextübergreifend lösen zu können.[31] Eine starke KI gibt es (noch) nicht[32], weshalb sich die Ausführungen dieser Arbeit auf die schwache KI beschränken. Außerhalb des juristischen Kontextes werden die Begriffe der starken oder schwachen KI allerdings kaum verwendet.

Vielmehr sind – wenn von KI die Rede ist – in aller Regel Methoden des maschinellen Lernens gemeint. [33] Von maschinellem Lernen spricht man, wenn man einen Computer so programmiert, dass er bestimmte Muster in Datensätzen erkennen kann und so ein Ergebnis errechnen kann. [34] Der Lernvorgang besteht darin, dass die relevanten Kriterien (Parameter) auf Grundlage der Trainingsdaten und Erfahrungswerte aus der Vergangenheit optimiert und angepasst werden.[35] Ähnlich definiert *Mitchell* den Begriff des

---

[27] Vgl. *Nink*, Justiz und Algorithmen, 2021, S. 210; *Wischmeyer*, AöR 143 (2018), 1, 17.

[28] *Wischmeyer*, AöR 143 (2018), 1, 17.

[29] *Braegelmann/Kaulartz*, in: Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 4.

[30] *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 3.

[31] *Gärtner*, Smart HRM, 2020, S. 21.

[32] *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 2; *Wischmeyer*, AöR 143 (2018), 1, 15.

[33] *Gärtner*, Smart HRM, 2020, S. 21; *Kossen/Kuruc/Müller*, in: Kerstin/Lampert/Rothkopf (Hrsg.), Wie Maschinen lernen, 2019, S. 3, 4; *Rostalski*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 251; *Wischmeyer*, AöR 143 (2018), 1, 12.

[34] Vgl. *Alpaydin*, Maschinelles Lernen, 3. Aufl. 2022, S. 3; *Gärtner*, Smart HRM, 2020, S. 22

[35] *Alpaydin*, Maschinelles Lernen, 3. Aufl. 2022, S. 3 f.

maschinellen Lernens: „A computer program is said to learn from experience *E* with respect to some tasks *T* and performance measure *P*, if its performance at tasks in *T*, as measured by *P*, improves with experience *E*."[36]

Um ein Modell zu entwickeln, das mit Methoden des maschinellen Lernens zustande kommt, werden die für die Entwicklung notwendigen Daten in ein Trainingsdatenset, ein Validierungs- und ein Testdatenset unterteilt.[37] Auf der Basis von Trainingsdaten bauen Lernalgorithmen ein Modell auf. Wenn ein maschinell lernendes System handgeschriebene Zahlen z. B. von 0-9 einordnen soll, benötigt es als Trainingsdaten viele verschiedene handgeschriebene Zahlen. Der Lernalgorithmus erkennt Muster, Beziehungen und Gesetzmäßigkeiten in den jeweiligen Daten und verallgemeinert sie.[38] Diese Verallgemeinerung ist notwendig, um das maschinell lernende System auf unbekannte Daten anzuwenden.[39] Lernalgorithmen benötigen numerische Werte, sodass stets alle Eingabewerte in numerische Zahlen umgewandelt werden müssen.[40] Die Validierungsdaten dienen dazu, das maschinell lernende System zu evaluieren und zu optimieren.[41] Die Testdaten sind für die finale Evaluierung da. Dabei wird überprüft, ob das Modell bei bislang ungesehenen Daten die richtigen Vorhersagen trifft.[42] In dieser Arbeit wird der Begriff der Trainingsdaten als Oberbegriff verwendet und nicht weiter in Validierungs-

---

[36] *Mitchell*, Machine Learning, 1997, S. 2.

[37] *Jebur/Al-Jumeily/Aljanabi u.a.*, in: Berry/Mohamed/Yap (Hrsg.), Supervised and Unsupervised Learning for Data Science, 2020, S. 145, 150; *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 31, spricht von mindestens zwei Teilmengen.

[38] S. *Basu/Bhattacharyya/Tai-hoon*, IJSEA 2010, 23, 24; *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 21.

[39] *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 21.

[40] *Gärtner*, Smart HRM, 2020, S. 22.

[41] Vgl. *Jebur/Al-Jumeily/Aljanabi u.a.*, in: Berry/Mohamed/Yap (Hrsg.), Supervised and Unsupervised Learning for Data Science, 2020, S. 145, 150.

[42] *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 205, vgl. *Jebur/Al-Jumeily/Aljanabi u.a.*, in: Berry/Mohamed/Yap (Hrsg.), Supervised and Unsupervised Learning for Data Science, 2020, S. 145, 150.

und Testdaten unterteilt.[43] Trainings-, Validierungs- und Testdaten sind alles Daten, die notwendig sind, um ein maschinell lernendes System zu erstellen oder ständig zu trainieren, damit es sich weiter verbessert. [44] Eine Unterscheidung ist für den rechtlichen Kontext daher nicht notwendig.[45]

I. Lernstile

Bevor das maschinelle Lernen näher anhand des neuronalen Netzwerks erklärt wird, folgt zunächst eine Einführung in die verschiedenen Lernstile. Sie werden vor allem in drei Kategorien unterteilt: überwachtes, unüberwachtes und bestärkendes Lernen.[46] Welcher Algorithmus des maschinellen Lernens angewendet wird, hängt davon ab, welches Problem gelöst werden soll und welche Daten vorliegen.[47] Bezweckt man etwa, bestimmte Daten einer Klasse zuzuordnen, z. B. ob man Bewerberinnen zum Gespräch einlädt oder sie bereits in der ersten Runde ablehnt, handelt es sich um ein Klassifikationsproblem.[48]

1. Überwachtes Lernen

Beim überwachten Lernen (sog. *supervised learning*) wird der Algorithmus mit Trainingsdaten „gefüttert", die auch immer die relevante Information, also das gewünschte Ergebnis, enthalten.[49] Der Algorithmus wird etwa mit vielen Bildern von Ottern und Bibern angelernt, wobei vorgegeben wird, um welche Tierart es sich beim jeweiligen Bild handelt. Nach dem Training des Algorithmus wird anhand von Test- und Validierungsdaten überprüft, wie

---

[43] So auch: *Hornung*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 91, 95.

[44] Nicht eingegangen wird auf den Schutz von Trainingsdaten durch das Immaterialgüterrecht, s. dazu etwa *Bartke/Hoffmann/Skiebe*, RDi 2022, 431-439.

[45] S. dazu auch: *Hornung*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 91, 95.

[46] *Gärtner*, Smart HRM, 2020, S. 22.

[47] *Ders.*, Smart HRM, 2020, S. 25.

[48] *Gesellschaft für Informatik*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, 2018, S. 30.

[49] *Buxmann/Schmidt*, Künstliche Intelligenz, 2018, S. 10.

exakt der Algorithmus die jeweiligen Daten einordnen kann. Ziel des Trainings ist es, dass das Entscheidungsmodell möglichst wenige Fehler macht.[50]

2. Unüberwachtes Lernen

Anders als beim überwachten Lernen soll der Algorithmus beim unüberwachten Lernen (sog. *unsupervised learning*) ein Muster in den ihm zur Verfügung gestellten Daten erkennen und eigenständig Kategorien bilden.[51] Um das oben genannte Beispiel wieder aufzugreifen: Bei Tierbildern von Ottern und Bibern werden dem Algorithmus keine Vorgaben über die Einteilung in zwei Gruppen gemacht. Das soll der Algorithmus selbst schaffen. Die wichtigste Lernmethode des unüberwachten Lernens ist das sog. Clustering.[52] Je nachdem, wie ähnlich sich die Objekte aufgrund ihrer Daten sind, werden sie in entsprechende Gruppen eingeteilt, sodass sich die Daten innerhalb einer Klasse oder eines Clusters stark ähneln.[53]

3. Verstärkendes Lernen

Beim verstärkenden Lernen (sog. *reinforcement learning*) soll der Algorithmus für ein Problem eine optimale Strategie erlernen.[54] Das implementierte Modell verbessert sich selbst, indem es für die Ergebnisse ein Feedback erhält.[55] Der Algorithmus erhält keinerlei Vorgaben oder konkrete Korrekturen, sondern lernt durch eigene Erfahrungen.[56] Das maschinell lernende System erhält aber eine Note (sog. *reward*) dafür, wie es sich

---

[50] *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 28.

[51] *Buxmann/Schmidt*, Künstliche Intelligenz, 2018, S. 10.

[52] *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 41.

[53] *Gärtner*, Smart HRM, 2020, S. 24; *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 41.

[54] *Martini*, Blackbox Algorithmus, 2018, S. 16; *Buxmann/Schmidt*, Künstliche Intelligenz, 2018, S. 10.

[55] *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 10.

[56] *Gärtner*, Smart HRM, 2020, S. 24.

verhalten hat. Es bekommt aber keinen exakten Hinweis dafür, was sich genau verbessern soll: Nur die Ziele, nicht die Lösungswege werden vorgegeben.[57]

Anschaulich ist das von *Gärtner* entwickelte Beispiel für ein Szenario des verstärkenden Lernens: Wird am Ende einer Taxifahrt kein Trinkgeld gegeben, könnte der Taxi-Algorithmus es als Hinweis erkennen, dass die Fahrt nicht optimal war. Er muss herausfinden, welche Aktionen dafür verantwortlich waren. Vielleicht wurden die Vorfahrtsregeln missachtet oder es wurde nicht die schnellste Route gewählt. Der Vorgang wird so oft wiederholt, bis der Vorhersagefehler des Algorithmus gegen Null tendiert und schließlich vorhersehbar ist, bei welchen Aktionen ein Trinkgeld gegeben wird.[58]

II. Künstliche neuronale Netze

Eine Lernaufgabe des überwachten Lernens ist – wie bereits erwähnt – die Klassifikation. Setzt man algorithmische Entscheidungssysteme bei der Personalauswahl ein, dienen sie häufig der Klassifizierung, etwa von Arbeitnehmerinnen oder Bewerberinnen: Diese Systeme sollen dabei helfen, ob jemand eingestellt, befördert, abgelehnt oder nicht befördert wird. Die Klassifikation kann z. B. durch den Einsatz eines neuronalen Netzes erfolgen. Es gibt viele verschiedene Arten künstlicher neuronaler Netze[59], auf die im Einzelnen nicht eingegangen werden kann. Für die Zwecke dieser Arbeit reicht es aus, lediglich einen Überblick über die grundsätzliche Funktionsweise eines neuronalen Netzes aufzuzeigen. Neuronale Netze werden hier aus dem Grund vorgestellt, weil sie mittlerweile die „vorherrschende [...] Erscheinungsform des maschinellen Lernens" sind.[60]

---

[57] *Hoppe*, in: Hartmann (Hrsg.), KI & Recht kompakt, 2020, S. 1, 14.

[58] *Gärtner*, Smart HRM, 2020, S. 24.

[59] *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen, 2018, S. 11.

[60] *Martini*, Blackbox Algorithmus, 2018, S. 24; vgl. *Niederée/Nejdl*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 2 56 f.; *Söbbing*, MMR 2021, 111.

1. Aufbau eines künstlichen neuronalen Netzes

Mithilfe eines neuronalen Netzes kann man ein maschinell lernendes System entsprechend trainieren, sodass es etwa handschriftliche Zahlen erkennt. Damit ein solches System Bilder lesen kann, müssen sie zunächst in Pixel übersetzt werden.[61] Schwarze Pixel erhalten etwa den Wert „0“, weiße Pixel den Wert „1“.[62]

Abbildung entnommen aus: *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 133

Vorstellen kann man sich ein neuronales Netz wie folgt[63]: Es besteht aus mehreren Schichten (sog. *layer*), die wiederum aus einzelnen „Neuronen“ bestehen. In der Eingabeschicht (sog. *input layer*) werden je nach *Input* bestimmte Neuronen aktiviert, die wiederum Neuronen in der nächsten (verborgenen) Schicht (sog. *hidden layer*) aktivieren. Der *Output* einer Schicht ist jeweils der *Input* für die nächste Schicht.[64] Die Aktivierung der einzelnen Neuronen wird mithilfe einer Aktivierungsfunktion vorgenommen. Diese Funktion beinhaltet die einzelnen Parameter eines Neurons, die entsprechend gewichtet sind. Wenn ein bestimmter Schwellenwert erreicht wird, werden die entsprechenden Neuronen in der nächsten Schicht aktiviert.[65] Man kann sich das künstliche neuronale Netz mithin auch ähnlich wie einen Filter vorstellen: Steht am Anfang eine Eingabe, soll am Ende ein konkretes Ergebnis herausgefiltert werden. Die letzte Schicht ist die Ausgabeschicht (sog. *output*

---

[61] *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 132.

[62] *Dies.*, Data Science – was ist das eigentlich?!, 2018, S. 132; *Hoppe*, in: Hartmann (Hrsg.), KI & Recht kompakt, 2020, S. 1, 11.

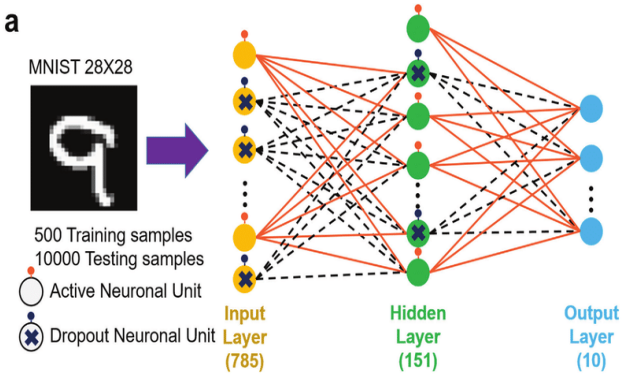
[63] Zur ausführlichen Erklärung eines neuronalen Netzes s. *Alpaydin*, Maschinelles Lernen, 3. Aufl. 2022, S. 285 ff.; *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 285 ff.; s. außerdem: *Söbbing*, MMR 2021, 111.

[64] *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 135.

[65] Vgl. *Gärtner*, Smart HRM, 2020, S. 30.

layer). Besteht ein komplexes neuronales Netzwerk aus vielen Schichten, spricht man von *Deep Learning*.[66] Die mehrlagigen neuronalen Netze, die teilweise bis zu 1.000 Schichten beinhalten, sind komplex:[67] Ein Sprachmodell von Microsoft besteht etwa aus 105 Schichten und 530 Milliarden Parametern.[68]

Die folgende Grafik[69] zeigt ein neuronales Netzwerk. Als Input dient die handgeschriebene Ziffer 9. Die erste Schicht besteht aus 785 Neuronen, wobei je nach Eingabe Neuronen aktiviert werden, die wiederum andere Neuronen in den verborgenen Schichten aktivieren. In der letzten Schicht wird das Ergebnis angezeigt.



2. Lernprozess des neuronalen Netzes

Der Lernprozess[70] eines neuronalen Netzes würde beim Problem „Handschriftliche Zahlen erkennen" wie folgt ablaufen: In das neuronale

---

[66] *Gärtner*, Smart HRM, 2020, S. 30; *Gertz/Aumiller*, LTZ 2022, 31; *Schulz*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, 579.

[67] *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 322.

[68] *Alvi/Kharya*, Using DeepSpeed and Megatron to Train Megatron-Turing NLG 530B, the World's Largest and Most Powerful Generative Language Model, 2021, https://perma.cc/EJ45-79G3 (archiviert am 10.01.2023).

[69] Grafik von *Huang/Xiao/Yang/Yu/He/Whang/Guo*, Adv. Sci. 2020, 7, 2001842, https://perma.cc/5K7Z-KRZS (archiviert am 02.11.2022).

[70] S. dazu auch: *Ehinger/Stiemerling*, CR 2018, 761, 762; *Söbbing*, MMR 2021, 111, 112 f.; Braegelmann/Kaulartz/*Stiemerling*, S. 19 ff.; *Steven W. Knox*, in: Balding/Cressie/Fitzmarucie u.a. (Hrsg.), Wiley Series in Probability and Statistics, S. 65 ff.

Netz werden viele handschriftliche Zahlen eingepflegt und *Outputs* generiert. Ist die Vorhersage falsch, werden die Aktivierungskriterien so verändert, dass sich der Fehler reduziert. Dieser Vorgang wird *Backpropagation* genannt.[71] Der Lernprozess besteht deshalb im Wesentlichen darin, dass die Parameter und deren Gewichtung der einzelnen Verbindungen zwischen den Neuronen entsprechend angepasst werden. Die gelernten Verbindungen werden als Aktivierungsfunktion in den jeweiligen Neuronen eingespeichert.[72] Nach einer langen Trainingsphase sollte das neuronale Netz in der Lage sein, *Input-Signale* mit den richtigen *Output-Signalen* zu verknüpfen und die richtige Zahl zu erkennen.[73]

Wird etwa ein maschinell lernendes System trainiert, das zur Analyse der Persönlichkeitsmerkmale anhand des Big-Five-Modells[74] eingesetzt werden soll, könnte der Trainingsprozess so ablaufen, dass verschiedene Personen die verschiedenen Datensätze anhand des Big-Five-Modells einordnen und das System die entsprechenden Verbindungen zwischen eingepflegten Daten und Ergebnis lernt. Ein tatsächlich genutztes System zur Persönlichkeitsanalyse wurde mit mehr als 12.000 Daten trainiert, die von über 2.500 Personen entsprechend eingeordnet wurden.[75]

D. Zwischenergebnis: Algorithmische Systeme im Kontext dieser Arbeit

1. Algorithmische Systeme sind im Kontext dieser Arbeit Softwaresysteme, die Menschen bewerten und algorithmenbasiert Entscheidungen treffen.[76] Häufig kommen diese Systeme unter Einsatz

---

[71] *Ertel*, Grundkurs Künstliche Intelligenz, 5. Aufl. 2021, S. 305; *Steven W. Knox*, in: Balding/Cressie/Fitzmarucie u.a. (Hrsg.), Wiley Series in Probability and Statistics, S. 69 *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 138.

[72] *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 138.

[73] *Dies.*, Data Science – was ist das eigentlich?!, 2018, S. 138.

[74] S. dazu auch unter: Kapitel 2 A.III. (S. 26).

[75] Vgl. *Retorios* personality model, S. 3, https://perma.cc/6H8A-H3UV (archiviert am 25.02.2023). Inzwischen wird das Modell nicht mehr verwendet.

[76] Kapitel 1 A. (S. 9).

maschineller Lernmethoden zustande.[77] Systeme, die unter Einsatz maschineller Lernmethoden zustande gekommen sind, werden im Kontext dieser Arbeit als maschinell lernende Systeme oder (Hochrisiko)-KI-Systeme bezeichnet.

2. Bei den maschinellen Lernstilen wird zwischen überwachtem, unüberwachtem und verstärkendem Lernen differenziert.[78] Maschinelles Lernen beschreibt den Vorgang, dass ein Modell derart programmiert wird, dass es bestimmte Trainingsdaten analysiert und daraus Muster ableitet, sodass ein Algorithmus entsteht, der andere (unbekannte) Daten als die Trainingsdaten verarbeiten kann. Der Lernprozess besteht insbesondere darin, dass die relevanten Parameter des Modells auf Basis der Trainingsdaten und Erfahrungswerte optimiert werden. Nach Abschluss des Lernprozesses ist es für einen Menschen nicht ohne Weiteres verständlich, warum ein einzelner Parameter einen bestimmten Wert hat. Hierin liegt der Unterschied zu einem nicht-lernenden System, bei dem sämtliche Parameter händisch einprogrammiert werden.

3. Solche Systeme funktionieren ausschließlich nach unmittelbar von Menschen einprogrammierten Regeln im Sinne eines „Wenn-Dann-Schemas“. Auch solche nicht-lernenden Systeme fallen nach dem Verständnis dieser Arbeit unter die Definition eines algorithmischen Systems. Rechtliche Herausforderungen stellen sich aber insbesondere beim Umgang mit maschinell lernenden Systemen, sodass der Fokus der Untersuchung auf diesen Systemen liegt.

---

[77] Kapitel 1 C (S. 12).
[78] Kapitel 1 C.I. (S. 15).

Kapitel 2

Anwendungsszenarien

Acht von zehn Unternehmen sind der Meinung, dass durch eine Digitalisierung des Bewerbungsprozesses eine freie Stelle schneller besetzt werden könnte. [1] Über die Hälfte der Top 1.000 umsatzstärksten Unternehmen [2] aus Deutschland glaubt, dass offene Stellen dadurch passgenauer besetzt werden könnten. Vier von zehn Unternehmen sind der Meinung, dass der Bewerbungsprozess so außerdem fairer gestaltet werden könne.[3]

Es gibt bereits einige algorithmische Systeme, die man im Personalwesen nutzt. Nachfolgend werden Systeme vorgestellt, die im Bewerbungsverfahren, bei Beförderungen oder bei Kündigungen eingesetzt werden. Da es eine Vielzahl unterschiedlicher Systeme[4] gibt, wird nur eine Auswahl vorgestellt.

---

[1] *Laumer/Maier/Christian, Oehlhorn, Caroline u.a.*, Digitalisierung und Zukunft der Arbeit, 2020, S. 9.

[2] *Dies.*, Digitalisierung und Zukunft der Arbeit, 2020, S. 2.

[3] In der IT-Branche sind sogar drei Viertel der befragten Top 300 Unternehmen aus Deutschland dieser Meinung, vgl. *dies.*, Digitalisierung und Zukunft der Arbeit, 2020, S. 9.

[4] *Ajunwa*, SLU 2018, 21, 23 ff.; *Borgert/Helfritz*, Künstliche Intelligenz in HR, S. 9 ff.; *Bundesverband der Personalmanager*, Zwischen Euphorie und Skepsis, 2019, S. 13 ff.; *Ettl-Huber/Kummer/Trinkl u. a.* (Hrsg.), Artificial Intelligence und Digital Recruiting im Human Resource Management, 2021, S. 14 ff.; *Joos*, NZA 2020, 1216; *Lederer/Müller-Jungnickel/Pirkl*, in: Lichtenthaler (Hrsg.), Künstliche Intelligenz erfolgreich umsetzen, 2021, 46 f.; *Nawaz/Gomes*, IJACSA 2019, 1; *Waas*, RdA 2022, 125, 127.

A. Bewerbungsverfahren

Laut einer Studie von Bitkom Research aus dem Jahr 2018 erhalten Großunternehmen mit mindestens 500 Arbeitnehmerinnen im Schnitt ca. 2.000 Bewerbungen jährlich, Unternehmen mit 100-499 Arbeitnehmerinnen 370 Bewerbungen und kleinere Unternehmen mit 50-99 Arbeitnehmerinnen ca. 180 Bewerbungen. [5] Bei hohen Bewerberinnenzahlen ist es unter Umständen notwendig, dass zunächst eine Vorauswahl geeigneter Bewerberinnen getroffen wird. Andernfalls kann man der Menge an Bewerbungen womöglich kaum gerecht werden. [6] Zur Bewerberinnenvorauswahl werden unterschiedliche algorithmische Systeme eingesetzt.

I. *Recommender-Systeme* bei Karrierenetzwerken

Nach einer Studie des *Centre of Human Resources Information Systems* (CHRIS) im Auftrag der *Monster Worldwide Deutschland GmbH*, einem Online-Recruiting-Unternehmen, nutzt jedes zehnte Unternehmen in Deutschland sog. *Recommender-Systeme* [7] : Kandidatinnen erhalten Jobvorschläge und den Unternehmen werden neue Talente automatisiert vorgeschlagen. Der Software-Anbieter *Textkernel* ermöglicht Recruiterinnen, firmeneigene Datenbanken und externe soziale Netzwerke nach Kandidatinnen zu durchsuchen [8] : Die Software *Match*! wertet dabei die einzelnen Textbausteine aus und überprüft, inwieweit Kandidatinnen- und Stellenprofil zueinander passen.[9]

---

[5] *Bitkom*, Woran scheitern Einstellungen?, 2018, S. 5.

[6] Bei *Google* bewerben sich pro Jahr ca. drei Millionen Leute, ca. 6.000 Menschen werden tatsächlich eingestellt, s. *Akhtar/Gillett*, Business Insider, 12.4.2020, https://perma.cc/6LSN-QAQ4 (archiviert am 02.08.2022).

[7] *Laumer/Maier/Christian, Oehlhorn, Caroline u.a.*, Digitalisierung und Zukunft der Arbeit, 2020, S. 18.

[8] *Gärtner*, Smart HRM, 2020, S. 68; *Textkernel* s. https://perma.cc/YU7Q-ENY2 (archiviert am 09.01.2023).

[9] *Ders.*, Smart HRM, 2020, S. 68.

Auch bei der sozialen Arbeitsplattform *LinkedIn* hilft der *LinkedIn Recruiter*, Kandidatinnen zu finden, anzusprechen und zu verwalten.[10] Eine menschliche Recruiterin erstellt zunächst ein neues Projekt im *LinkedIn Recruiter* mit der zu besetzenden Stelle.[11] Die Software erstellt ein Ranking basierend auf Faktoren wie z. B. der Ort der Arbeitsstelle, Erfahrung in dem gesuchten Bereich und Grad der Wahrscheinlichkeit, dass eine Kandidatin antwortet.[12] Die Recruiterin kann sich das Profil einer empfohlenen Kandidatin anschauen, das Profil zu ihrem Projekt hinzufügen, um es später anzuschauen, oder der Kandidatin eine Nachricht via *LinkedIn* senden.

Der *Pocket Recruiter* sucht vollautomatisiert nach passenden Kandidatinnen.[13] Der Algorithmus durchsucht auf der Grundlage einer Stellenausschreibung interne Datenbanken und *Social-Media*-Plattformen, um die passende Kandidatin zu finden.[14]

Die Firma *LogOn* bietet ebenfalls eine Recruitingsoftware an, die Kandidatinnen und Unternehmen zusammenführt.[15] Nach dem Hochladen einer Stellenanzeige sucht die Software nach Kandidatinnen und erstellt eine Liste mit sog. *Matching*-Werten, d. h. wie gut die Kandidatin für die Stelle geeignet ist.

II. Chatbots

Ein Chatbot kann bei Fragen rund um die Bewerbung und auch zur Bewerbung selbst eingesetzt werden. Chatbots können Bewerberinnen etwa dabei unterstützen, die passende Stelle auf Basis von allen verfügbaren Stellen im Unternehmen zu finden.[16] Die Vorteile eines Chatbots sind vielfältig: Sie

---

[10] Zum *LinkedIn Recruiter* s. https://perma.cc/GET8-9TVS (archiviert am 02.08.2022).

[11] *Guo/Geyik/Ozcaglar u.a.*, The AI Behind LinkedIn Recruiter search and recommendation systems.

[12] *Dies.*, The AI Behind LinkedIn Recruiter search and recommendation systems.

[13] *Verhoeven* (Hrsg.), Digitalisierung im Recruiting, 2020, S. 122; Pocket Recruiter, https://perma.cc/85NS-PZVM (archiviert am 02.08.2022).

[14] *Ders.*, Digitalisierung im Recruiting, 2020, S. 122.

[15] S. *LogOn.technologies*, https://perma.cc/MU4M-G3J4 (archiviert am 02.08.2022).

[16] *Kohne/Kleinmanns Philipp/Rolf u.a.*, Chatbots, 2020, S. 23; s. etwa den Chatbot von assono: https://perma.cc/ZK4M-XR7Q (archiviert am 09.01.2023).

sind ständig verfügbar, sie sind nicht voreingenommen, die Bewerbungsprozesse werden verkürzt und es können erhebliche Kosten eingespart werden.[17] Nach einer Umfrage von *Hundertmark* geben die Befragten an, dass die Kundinnenzufriedenheit steigt, wenn ein Chatbot eingesetzt wird.[18] Ein Grund dafür liegt vermutlich darin, dass Recruiterinnen durch den Einsatz eines Chatbots hinsichtlich allgemeiner Fragen entlastet werden und sich stärker darauf konzentrieren, sich intensiver mit persönlicheren Fragen an die Bewerberinnen zu wenden.

III. Persönlichkeitsbewertung mithilfe von Video- oder Sprachanalysen

Eine weitere Möglichkeit, geeignete Kandidatinnen für einen Posten zu finden, ist eine Persönlichkeitsbewertung mithilfe einer Video- oder Sprachanalyse.[19]

Die Software *Precire* des gleichnamigen Unternehmens soll die Wirkung von Sprache objektiv prognostizierbar und messbar machen.[20] Die Sprachanalyse kann nach Angaben des Unternehmens etwa Aufschluss darüber geben, wie teamfähig, ehrgeizig, belastbar oder verantwortungsbereit eine Bewerberin ist.[21] Das Unternehmen wurde stark kritisiert und gewann 2019 den „Big Brother Award" – ein Negativpreis für Unternehmen mit zweifelhaftem Umgang mit Daten.[22] Gerügt wurde insbesondere, dass es keine gute Dokumentation des methodischen Vorgehens gegeben habe und auch nicht belegt worden sei, inwiefern *Precire* gegenüber herkömmlichen Fragebögen

---

[17] *Verhoeven* (Hrsg.), Digitalisierung im Recruiting, 2020, S. 103, 106.

[18] *Hundertmark*, Chatbot Umfrage DACH 2020, Statista: https://perma.cc/5TF2-ESP8 (archiviert am 02.08.2022).

[19] *Greb/Linnenbürger*, in: Gourmelon (Hrsg.), Personalauswahl – ein Blick in die Zukunft, 2018, S. 75; *Havlíková*, DSRITB 2020, 141; *Cynthia C. S. Liem/Markus Langer/Andrew M Demetriou u.a.*, in: Escalante/Escalera/Guyon u.a. (Hrsg.), Explainable and Interpretable Models in Computer Vision and Machine Learning, 2018, S. 197.

[20] Nähere Informationen zu *Precire* s. https://precire.com/technologie/ (zuletzt abgerufen am 19.01.2021).

[21] *Geißler*, in: Kramer (Hrsg.), Kramer IT-ArbR, 2019, B. Rn. 1082.

[22] *Bös*, Precire findet einen Käufer, FAZ 03.03.2021, https://perma.cc/93X2-W3DF (archiviert am 02.08.2022).

besser geeignet sei.[23] Mittlerweile wurde das Unternehmen an die *4 Technology Group* verkauft und existiert daher nicht mehr in der ursprünglichen Form.[24]

Die Software *Seedlink* funktioniert ähnlich: Anhand einer Sprachanalyse von drei kompetenzbasierten Fragen empfiehlt sie der Recruterin eine Bewerberin.[25] Die Software analysiert die Sprache im Hinblick auf u.a. Syntax und Wortwahl.[26] Danach ist es möglich, Aussagen über die Persönlichkeit, Fähigkeiten und Werte der Person zu treffen.[27] Weniger als 150 Worte sollen genügen, um ein Persönlichkeitsprofil nach *Big Five* – im Englischen als OCEAN-Modell bezeichnet – und DISG (engl.: DISC) zu generieren.[28] Das *Big Five* Modell ordnet jeden Menschen anhand bestimmter Persönlichkeitsmerkmale ein. Die fünf großen Persönlichkeitsmerkmale sind: Offenheit (*openness*), Gewissenhaftigkeit (*conscientiousness*), Extraversion (*extraversion*), Verträglichkeit (*agreeableness*) und Neurotizismus (*neuroticism*).[29] Das DISG-Persönlichkeitsmodell beruht hingegen auf vier wesentlichen Merkmalen: Dominanz (*dominance*), Initiative (*influence*), Stetigkeit (*steadiness*) und Gewissenhaftigkeit (*conscientiousness*). [30] Das Unternehmen L'Oréal beispielsweise setzte *Seedlink* ein, um Praktikantinnen auszuwählen.[31] *Seedlink* existiert allerdings in der ursprünglichen Form auch nicht mehr; jedenfalls findet man online keine Informationen mehr über das Unternehmen und die Software.

---

[23] *Schwertfeger*, Sprachanalyse Precire: Durchgefallen, Wirtschaftspsychologie heute, 26.07.2019, https://perma.cc/LQ52-ER7L (archiviert am 16.01.2023).

[24] *Bös*, Precire findet einen Käufer, FAZ 03.03.2021, https://perma.cc/93X2-W3DF (archiviert am 02.08.2022).

[25] S. *Seedlink Sciene*, https://perma.cc/F98Z-HC6T (archiviert am 02.08.2022).

[26] S. *Greple*, https://perma.cc/785N-L6DX (archiviert am 02.08.2022).

[27] S. *Seedlink Science*, https://perma.cc/F98Z-HC6T (archiviert am 02.08.2022).

[28] S. *Greple*, https://perma.cc/785N-L6DX (archiviert am 02.08.2022).

[29] *Landge/Mahajan/Mahender*, in: Hassanien/Bhatnagar/Darwish (Hrsg.), Advanced Machine Learning Technologies and Applications, 2020, 703-712, 705 ff. f.

[30] *Dauth*, Führen mit dem DISG-Persönlichkeitsprofil, 2012, S. 18.

[31] *Queb Bundesverband*, KI und Sprachanalyse im Recruiting: L'Oréal setzt auf Seedlink, https://perma.cc/EM9M-W34F (archiviert am 02.08.2022).

Greple nutzt ebenfalls KI, um – nach eigener Aussage – bessere Personalentscheidungen zu treffen.[32] *Greple* bietet verschiedene Produkte an, z. B. einen „Cultural Fit Test", mit dem man herausfinden kann, ob und wie gut Kandidatinnen zum Unternehmen passen.

Die Firma *HireVue* [33] bietet hauptsächlich eine Videoauswertung an. Bewerberinnen beantworten Fragen in einer Videoaufnahme, welche im Hinblick auf Gestik, Mimik, Veränderungen in der Stimme und Blickwechsel genau analysiert wird. [34] Auch hier wird wieder das *Big Five* Persönlichkeitsmodell als Grundlage für die Analyse genommen. Eine ähnliche Technologie bot während der Erstellung dieser Arbeit auch die Firma *Retorio* an.[35] Inzwischen setzt *Retorio* dagegen ausschließlich auf KI-basierte Coaching-Angebote.[36]

IV. *„Background-Checks"* mithilfe algorithmischer Systeme

Um zu prüfen, ob Angaben in einem Lebenslauf wahrheitsgetreu sind, nehmen Arbeitgeberinnen bei potenziellen neuen Arbeitnehmerinnen sog. *Background-* oder *Pre-Employment-Checks* vor. [37] Das Unternehmen *First Advantage* bietet Background Checks an. Die Software überprüft im Lebenslauf etwa die Ausbildungsstationen und sucht in sozialen Netzwerken nach Informationen über die Kandidatinnen.[38]

---

[32] *Greple*, https://perma.cc/D8CN-8CGQ (archiviert am 02.08.2022).

[33] *Hire Vue*, https://perma.cc/649W-92H6 (archiviert am 02.08.2022).

[34] *Verhoeven* (Hrsg.), Digitalisierung im Recruiting, 2020, S. 122.

[35] *Retorio*, https://perma.cc/D63P-TN54 (archiviert am 02.08.2022).

[36] *Retorio*, https://perma.cc/VPZ7-DQ9D (archiviert am 10.12.2023).

[37] *Hauer/Raudonat/Zweig*, Anwendungsszenarien: KI-Systeme im Personal- und Talentmanagement, 2020, S. 13.

[38] *First Advantage*, https://perma.cc/67YM-QMGA (archiviert am 02.08.2022).

B. Beförderung

I. Interne Bewerbungsprozesse

Eine Studie der Jobplattform *Stepstone* zeigt, dass 34,6 % der Arbeitnehmerinnen aufgrund fehlender Aufstiegsmöglichkeiten kündigen.[39] Sowohl für die Arbeitgeberin als auch für die Arbeitnehmerin ist es mithin wichtig, dass eine gute Beförderungsstruktur im Unternehmen besteht.[40] Einerseits ist das Erhalten und Fördern von Arbeitnehmerinnen kostengünstiger als eine hohe Wechselquote ebendieser: Die durchschnittlichen Fluktuationskosten pro Stelle belaufen sich auf 14.900 Euro.[41] Andererseits wirkt es sich positiv auf die Arbeitsleistung aus, wenn die Arbeitnehmerinnen Wertschätzung erfahren und auch Anreize für eine Beförderung gesetzt werden.[42]

Das Unternehmen *IBM* bietet unter anderem sog. *Talent development services* an. Darunter fällt z. B. KI einzusetzen, um eine vorausschauende Personaleinsatzplanung zu ermöglichen, Talente zu suchen oder KI-gestützte Bots einzusetzen, die als vertrauenswürdige Personalberaterinnen für Arbeitnehmerinnen eingesetzt werden sollen. *IBM* hilft Unternehmen dabei, eine Strategie für Talentmanagement zu erstellen. Dabei ist *IBM* der Auffassung, dass traditionelle Einstellungs- und Schulungsmechanismen nicht mehr ausreichen würden. Vielmehr müssten Unternehmen individuell herausfinden und bewerten, welche Kenntnisse und Kompetenzen ihre Arbeitnehmerinnen brauchen. *IBM* nutzt KI, personalisierte Empfehlungen, digitale Zertifizierungen und sog. *Design Thinking*, damit eine Kultur der

---

[39] *Nier*, Warum Beschäftigte kündigen, Statista, 24.09.2019, https://perma.cc/KJ8M-RLHA (archiviert am 02.08.2022).

[40] Vgl. *Ettl-Huber/Kummer/Trinkl u. a.* (Hrsg.), Artificial Intelligence und Digital Recruiting im Human Resource Management, 2021, S. 50, die AI auch als Chance sieht, die Wechselwilligkeit der Arbeitnehmerinnen festzustellen.

[41] *Jacob/Kyaw*, in: Gärtner (Hrsg.), Smart Human Resource Management, 2020, S. 53, 58; *Warmbrunn*, Mitarbeiter-Lebenszyklus: Personalmanagement nach individuellem Maß, Sage Blog, 14.10.2019, https://perma.cc/P3YK-4JBD (archiviert am 02.08.2022).

[42] Vgl. *Ettl-Huber/Kummer/Trinkl u. a.* (Hrsg.), Artificial Intelligence und Digital Recruiting im Human Resource Management, 2021, S. 50, die beschreibt, dass man mit KI-Anwendungen etwa einen Burnout frühzeitig erkennen könne.

ständigen Kommunikation und Weiterqualifizierung im Unternehmen aufgebaut wird.[43]

II. Leistungsbewertungssysteme

Um die Leistung der Arbeitnehmerinnen zu ermitteln, kann man Leistungsbewertungssysteme einsetzen, um Arbeitnehmerinnen regelmäßig Feedback zu ihrer Arbeit zu geben. Die Personalsoftware *Zonar* von *Zalando* bewertete Arbeitnehmerinnen: Auf Basis hochfrequenter Echtzeitbewertungen und periodischer Beurteilungen der Arbeitnehmerinnen wurden die Arbeitnehmerinnen in die Kategorie sog. Low-, Good- oder Top-Performer eingestuft.[44] Anhand der Einteilung wurden individuelle Bewertungsgespräche strukturiert, betriebliche Aufstiegsoptionen verteilt und Lohnsteigerungen gewährt oder versagt.[45] Die Software wurde erheblich kritisiert: Die Überwachung war allgegenwärtig, weshalb das Betriebsklima insgesamt sehr schlecht war.[46] Alle erhobenen Informationen wurde ohne Einwilligung gespeichert und waren dem Unternehmen dauerhaft zugänglich.[47] Ob und wie sie heute eingesetzt wird, lässt sich nicht eindeutig herausfinden.

Auch werden andere maschinell lernende Systeme eingesetzt, die etwa kontrollieren, ob man tatsächlich arbeitet und nicht das Mobiltelefon während der Arbeit nutzt.[48] In Lagerhäusern und Vertriebszentren kann ein System etwa die Produktivität kontrollieren, indem durch sog. *wearables*[49] gemessen wird, wie lange sich eine Arbeitnehmerin in einem bestimmten Bereich aufgehalten hat.[50] *Wearables* sind Kleincomputer, die am Körper

---

[43] S. https://perma.cc/KS4B-AWGY (archiviert am 02.08.2022); weiterführende Informationen zu IBM *Verhoeven* (Hrsg.), Digitalisierung im Recruiting, 2020, S. 121 f.

[44] *Staab/Geschke*, Ratings als arbeitspolitisches Konfliktfeld, 2020, S. 19.

[45] *Dies.*, Ratings als arbeitspolitisches Konfliktfeld, 2020, S. 10.

[46] S. dazu umfassend *dies.*, Ratings als arbeitspolitisches Konfliktfeld, 2020, S. 27 ff.

[47] *Dies.*, Ratings als arbeitspolitisches Konfliktfeld, 2020, S. 28.

[48] *Waas*, RdA 2022, 125, 127.

[49] S. dazu: *Ajunwa*, SLU 2018, 21, 34 ff.; *Blinn*, DSRITB 2016, 519.

[50] S. dazu etwa den Einsatz von *Wearable Sensors* bei *DHL*: https://perma.cc/E37Q-JYEA (archiviert am 25.02.2023).

getragen werden.[51] Die Einsatzfelder sind vielfältig: Etwa können durch Aufzeichnungen, wo sich eine Person befindet, Warnungen ausgesprochen werden, wenn in einer Betriebsanlage ein Unfall zwischen einem Fußgänger und einem Gabelstapler droht.[52]

Schließlich können algorithmische Systeme konkrete Weisungen erteilen.[53]

C. Kündigung

Die Kündigung einer Arbeitnehmerin ist kostenintensiv und bedeutet einen Effizienz- und Wissensverlust. Es ist deshalb für die Arbeitgeberin attraktiv, frühzeitig Maßnahmen zu ergreifen, wenn Arbeitnehmerinnen unzufrieden sind.[54] Das Start-Up *Predict42* berechnet neben der Kündigungswahrscheinlichkeit von Arbeitnehmerinnen auch die Kosten, die normalerweise mit einer Kündigung einhergehen („*cost of attrition*").[55]

IBM benutzt ein System namens *Predictive Attrition Program*, welches mit einer Genauigkeit von 95 % vorhersagt, welche Arbeitnehmerinnen kündigen werden.[56]

Außerdem gibt es auch Systeme für die Sozialauswahl bei der betriebsbedingten Kündigung durch die Arbeitgeberin. *CMS Select* liefert anhand von zahlreichen BAG- und LAG-Urteilen Vorschläge für die Sozialauswahl.[57].

---

[51] *Blinn*, DSRITB 2016, 519; *Götz*, Big Data im Personalmanagement, 2020, S. 29 f.; *Kopp/Sokoll*, NZA 2015, 1352.

[52] S. dazu etwa den Einsatz von *Wearable Sensors* bei *DHL*: https://perma.cc/E37Q-JYEA (archiviert am 25.02.2023).

[53] *Waas*, RdA 2022, 125, 127; umfassend dazu s. *Knitter*, Digitale Weisungen, 2022.

[54] *Hauer/Raudonat/Zweig*, Anwendungsszenarien: KI-Systeme im Personal- und Talentmanagement, 2020, S. 21.

[55] *Predict 42*, https://perma.cc/6ZAW-2BJV (archiviert am 02.08.2022).

[56] *Wennker*, Künstliche Intelligenz in der Praxis, 2020, S. 62.

[57] *CMS Select*, https://perma.cc/S358-TWCY (archiviert am 02.08.2022).

D. Zwischenergebnis: Kein flächendeckender Einsatz in Deutschland

1. Der Überblick zeigt, dass es bereits eine Vielzahl an algorithmischen Systemen gibt, die im Bewerbungsprozess oder im bestehenden Arbeitsverhältnis eingesetzt werden können. Der größte Einsatzbereich algorithmischer Systeme ist hier bei der Vorauswahl von Bewerberinnen.[58]

2. Dennoch werden algorithmische Systeme in Unternehmen in Deutschland nicht flächendeckend eingesetzt: 11 % der Unternehmen mit mehr als fünfzig Arbeitnehmerinnen in Deutschland setzen KI ein, 15 % diskutieren den Einsatz von KI. In den großen Unternehmen ab 500 Arbeitnehmerinnen wiederum setzen 22 % der befragten Unternehmen KI bereits ein. Diese Ergebnisse brachte eine Studie aus dem Jahr 2020 des *TÜV Verbands* hervor.[59] Bei der Einstellung von Arbeitnehmerinnen nutzen laut einer Studie von *Adesso* 23 % von über 2.000 befragten Unternehmen in Deutschland sog. KI-Systeme.[60]

3. In anderen Ländern ist der Einsatz algorithmischer Systeme schon stärker verbreitet: Den Anbieter *HireVue* etwa nutzen nach eigenen Angaben des Unternehmens über 800 Unternehmen weltweit, um Bewerbungsprozesse zu optimieren.[61] Auch das Unternehmen *Seedlink* hat seine KI-Software für Bewerbungsverfahren weltweit angeboten und hatte Kunden in über dreißig Ländern. Darunter waren namenhafte Unternehmen wie *Coca-Cola, L'Oréal* oder *Sephora*.[62]

---

[58] Vgl. *Statista Research Department*, In welcher Form könnten Sie sich den Einsatz von KI im Bewerbungsprozess vorstellen?, 21.07.2022, https://perma.cc/888E-YSLV (archiviert am 02.08.2022).

[59] *TÜV Verband*, Künstliche Intelligenz in Unternehmen, 2020, S. 10.

[60] *Adesso*, KI – eine Bestandsaufnahme, 2021, S. 28.

[61] *HireVue*, https://perma.cc/649W-92H6 (archiviert am 02.08.2022).

[62] *Seedlink Success Stories*, https://perma.cc/S26U-M54L (archiviert am 02.08.2022).

Kapitel 3

Menschliche und algorithmische Entscheidungen im Vergleich

Algorithmische Systeme – so die Hoffnung – können Benachteiligungen verringern und deshalb zu gerechteren Entscheidungen führen.[1] Es gibt aber auch einige Nachteile, die mit algorithmischen Entscheidungen einhergehen.[2] Im Folgenden werden wesentliche Unterschiede[3] zwischen menschlichen und algorithmischen Entscheidungen [4] herausgearbeitet, auf die im weiteren Verlauf der Arbeit immer wieder zurückgegriffen wird.

A. Objektivität und Determiniertheit

Algorithmische Systeme entscheiden immer auf Basis der vorgegebenen Regeln und sind nicht tagesformabhängig. [5] Menschliche Entscheidungen hingegen sind alles andere als objektiv.[6] Ein Lebenslauf kann einen stärkeren

---

[1] Kritisch: *Ernst*, VuR 2019, 401; differenziert: *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 16 ff.; *Zweig/Krafft*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, 204 ff.; überblicksartig zu Fragen rund um Legal Tech s. *Hähnchen/Schader/Weiler u.a.*, JuS 2020, 625;

[2] Statt vieler: *Blum*, People Analytics, 2021, S. 77 ff.; *Ernst*, in: Klafki/Würkert/Winter (Hrsg.), Digitalisierung und Recht, 2017, S. 63, 67 f.; *Dzida/Groh*, ArbRB 2018, 179; *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 17; *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen (2020).

[3] S. dazu etwa auch: *Spiekermann*, in: Mainzer (Hrsg.), Philosophisches Handbuch Künstliche Intelligenz, 2020.

[4] *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 16; vgl. *Zweig*, Wo Maschinen irren können, 2018, S. 15.

[5] *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 441.

[6] Ausführlich dazu: *Nink*, Justiz und Algorithmen, 2021, S. 28 ff.; s. dazu auch: *Zimmer/Stajcic*, NZA 2017, 1040.

Eindruck hinterlassen, wenn er kurz vor Feierabend gelesen wurde, Personalerinnen werden bewusst oder unterbewusst durch (diskriminierende) Vorurteile beeinflusst. [7] Zwar können auch bei rein menschlichen Entscheidungen Kriterien vorgegeben werden, nach denen die Entscheidung getroffen werden soll. [8] Bei Einstellungen können z. B. die vorherige Berufserfahrung, Sprachkenntnisse und soziale Kompetenz Kriterien sein. Dennoch wird sich die Person vermutlich (unterbewusst) von anderen Kriterien leiten lassen: Die Entscheidung eines Menschen kann von irrelevanten Faktoren abhängen, etwa wie hungrig die Person im Moment der Entscheidung war.[9]

Das ist bei einer algorithmischen Entscheidung nicht der Fall: Das algorithmische System kommt zu demselben Ergebnis unabhängig davon, ob es ein sonniger oder regnerischer Tag ist, ob es Morgen oder Abend ist oder ob sich jemand gestritten hat.[10] Die menschliche Entscheidung ist also „weniger determinierbar und stets anfällig für kognitive Fehlleistungen“ [11]. Auf den ersten Blick sind algorithmische Entscheidungen daher im Gegensatz zu menschlichen Entscheidungen objektiv.[12]

Auch algorithmische Systeme können zu diskriminierenden Ergebnissen führen. Grund dafür kann unter anderem sein, dass sie von Menschen programmiert werden und deren subjektive Auffassung widerspiegeln.[13] Dem kann man jedoch gezielt entgegenwirken, indem man an der Konzeption des Systems mehrere Entscheidungsträgerinnen beteiligt und allgemeine Standards für das Entscheidungssystem entwickelt.[14] Neben dem Aspekt, dass

---

[7] *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 14.

[8] *Ernst*, JZ 2017, 1026, 1028.

[9] Dazu ausführlich *Nink*, Justiz und Algorithmen, 2021, S. 74 f.

[10] S. *Zweig*, Wo Maschinen irren können, 2018, S. 15.

[11] *Ernst*, JZ 2017, 1026, 1028.

[12] *Nink*, Justiz und Algorithmen, 2021, S. 167; *Zweig*, Wo Maschinen irren können, 2018, S. 15.

[13] Vgl. *Herder*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, 183.

[14] *Bär*, Algorithmic Bias: Verzerrungen durch Algorithmen verstehen und verhindern, 2022, Teil III und IV, S. 125 ff.; vgl. *Datenethikkommission*, Gutachten der Datenethikkommission, 2019; s. umfassend dazu auch: *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 29 ff.

die Ergebnisse der Systeme durch die Programmiererinnen beeinflusst werden, gibt es weitere Ursachen für diskriminierende Entscheidungen. Darauf wird im dritten Teil der Arbeit näher eingegangen, wenn es darum geht, dass algorithmische Systeme AGG-konform eingesetzt werden müssen.[15]

B. Auswertung großer Datenmengen

Algorithmische Systeme können größere Datenmengen schneller analysieren, als Menschen je dazu in der Lage wären.[16] So können Probleme schneller, präziser und günstiger gelöst werden: Beispielsweise hat ein algorithmisches System zur Schülerinnenverteilung in New York dazu geführt, dass sich die Zahl von 31.000 Schülerinnen, die nicht einer weiterführenden Schule (*High School*) zugeteilt werden konnten, auf 3.000 Schülerinnen reduzierte.[17] Ziel des Algorithmus war es, etwa 80.000 Schülerinnen der *Middle School* der passenden *High School* zuzuordnen.[18] Schülerinnen der achten Klasse reichten eine Bewerbung ein, in der sie bis zu zwölf *High Schools* in der präferierten Reihenfolge auflisteten. Die *High Schools* erhielten Vorschläge von Schülerinnen und schlugen nach ihren Kriterien den besten Schülerinnen abhängig von der Anzahl der verfügbaren Plätze ein Angebot vor; alle anderen wurden abgelehnt. Schülerinnen mit Angeboten wurden aus der Liste entfernt, die Schülerinnen ohne Angebot durchliefen dieselbe Prozedur mit der von ihnen gerankten nächsten *High School*. Das Verfahren wurde so lange wiederholt, bis alle zwölf gelisteten *High Schools* kontaktiert wurden. Die *High Schools* erfuhren dabei nicht, auf welchem Platz die betreffende Schülerin sie gerankt hatte.

Bewerben sich auf eine Stelle viele Menschen, würde eine automatisierte Vorauswahl regelmäßig dabei helfen, die Bewerbungen zu sichten. Bei *Google*

---

[15] S. Kapitel 8 (S. 281).

[16] *Krüger/Lischka*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, 441; KI bietet etwa große Chancen in der Krebsforschung s. Artikel zu Krebsregisterdaten https://perma.cc/8C5A-SDXX (archiviert am 02.01.2023).

[17] *Dies.*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, 442.

[18] New York Independent Budget Office, https://perma.cc/93GR-F66P (archiviert am 09.01.2023).

etwa ist die Zahl derBewerbungen hoch. 2014 lag die Annahmequote bei 0,2 %; auf ca. 6.000 Stellen hatten sich drei Millionen Menschen beworben.[19]

C. Keine Berücksichtigung individueller Merkmale und Korrelation

Algorithmische Systeme treffen ihre Entscheidung anhand der einprogrammierten Merkmale und auf Grundlage der eingepflegten Daten.[20]

Bei nicht-lernenden Systemen bleiben Merkmale, die individuell auftreten und für die Entscheidung ggf. bedeutsam sind, allerdings unberücksichtigt.[21] Sie agieren aufgrund des Wenn-Dann-Schemas nur sehr starr.

Entscheidet hingegen ein Mensch, können solche Merkmale situationsgerecht berücksichtigt werden, da menschliche Entscheidungen viel flexibler sind:[22] Würde eine Bewerberin aufgrund des knapp nicht erreichten Prädikatsexamens wegen der Vorgaben eigentlich nicht in Betracht kommen, könnte die Person, die die Auswahlentscheidung trifft, sie dennoch einstellen, wenn die Bewerberin im Vorstellungsgespräch durch andere Fähigkeiten überzeugt.[23]

Werden hingegen Methoden des maschinellen Lernens verwendet, kann das System nicht nur Muster in den Daten erkennen.[24] Es kann vor allem auch Schlussfolgerungen aus den Mustern ziehen und entsprechend sein Verhalten anpassen.[25] Werden die generierten Ergebnisse von Menschen dahingehend bewertet, ob das maschinell lernende System etwa zum richtigen oder falschen

---

[19] *Akhtar/Gillett*, Business Insider, 12.04.2020, https://perma.cc/6LSN-QAQ4 (archiviert am 02.08.2022).

[20] *Ernst*, JZ 2017, 1026, 1027.

[21] *Ders.*, JZ 2017, 1026, 1027.

[22] *Ders.*, JZ 2017, 1026, 1028; *Zweig*, Wo Maschinen irren können, 2018, S. 15.

[23] Vgl. *Zweig*, Wo Maschinen irren können, 2018, S. 15.

[24] *Martini*, Blackbox Algorithmus, 2018, S. 21; *Nink*, Justiz und Algorithmen, 2021, S. 204.

[25] *Martini*, Blackbox Algorithmus, 2018, S. 21; *Hoffmann-Riem*, AöR 142 (2017), 1, 3; *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 12.

Ergebnis gekommen ist, kann das maschinell lernende System sich anpassen: Wird z. B. ein neuronales Netz verwendet, können die Gewichtungen der Parameter geändert werden. Dadurch kann das maschinell lernende System Wissen generieren („lernen") und ist somit in der Lage, auch unbekannte Daten auszuwerten.[26] Dabei ist allerdings problematisch, dass es für einen Menschen häufig schwer nachvollziehbar und erklärbar ist, wie ein maschinell lernendes System zu einem bestimmten Ergebnis gekommen ist.[27]

Ein maschinell lernendes System trifft eine Entscheidung zudem nur aufgrund von Daten aus der Vergangenheit.[28] Menschliche Entscheidungen können hingegen auch Prognosen für die Zukunft wagen.[29]

Hinzu kommt, dass maschinell lernende Systeme stets auf der Grundlage von Korrelationen und nicht auf der Grundlage von Kausalitäten entscheiden.[30] Lernalgorithmen ziehen Parallelen zwischen ähnlich gelagerten Fällen und bewerten auf dieser Grundlage andere Fälle. Das kann in vielen Fällen zu Fehlinterpretationen führen. *Bäcker* und *Jansen* führen das Problem am Beispiel der Sprachdiagnostik aus[31]: Aus wissenschaftlichen Untersuchungen gehe hervor, dass eine aufkommende Depression sich auch in der Sprache zeige. Häufig würden negative Emotionen zunehmen, in der Sprache würde ein stärkerer Ich-Bezug auftauchen und soziale Themen würden zurückgehen. Ein maschinell lernendes System könnte auf dieser Grundlage Menschen, bei denen diese Merkmale auftauchen, als „depressiv" einordnen. Allerdings sei nicht automatisch jeder Mensch, der einen starken Ich-Bezug oder negative Emotionen in der Sprache aufweise, geneigt, „depressiv" zu sein. Eine

---

[26] *Nink*, Justiz und Algorithmen, 2021, S. 204.

[27] S. dazu: Kapitel 4 (S. 39).

[28] *Lauscher/Legner*, ZfDR 2022, 367, 371.

[29] Vgl. *Nink*, Justiz und Algorithmen, 2021, S. 170 f.

[30] *Beck*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, 6; *Martini*, Blackbox Algorithmus, 2018, S. 53; *Hoffmann-Riem*, AöR 142 (2017), 1, 13; *Müller*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 205, 215 f.; *Wischmeyer*, AöR 143 (2018), 1, 13.

[31] *Bäcker/Jansen*, in: Gourmelon (Hrsg.), Personalauswahl – ein Blick in die Zukunft, 2018, 109 ff.

Korrelation sagt nichts über die Kausalität aus, vielmehr kann der Zusammenhang auch rein zufällig sein.[32]

D. Zwischenergebnis: Vor- und Nachteile sowohl menschlicher als auch algorithmischer Entscheidungen

1. Bei der Vorfilterung einer Vielzahl von Bewerbungen sind algorithmische Systeme menschlichen Entscheidungen in bestimmter Hinsicht überlegen: Sie können einerseits große Datenmengen schneller analysieren. [33] Andererseits sind sie nicht tagesformabhängig und entscheiden anhand feststehender Regeln: Algorithmische Systeme lassen sich also nicht von äußeren Umständen beeinflussen und sind daher auf den ersten Blick objektiver als menschliche Entscheidungen.

2. Nicht-lernende Systeme können jedoch nicht flexibel agieren. Das ist zwar bei maschinell lernenden Systemen anders. Es besteht jedoch die Gefahr, dass maschinell lernende Systeme aufgrund bestimmter Korrelationen zwischen Merkmalen zu einem bestimmten Ergebnis kommen, obwohl keine Kausalität zwischen den Merkmalen besteht.[34] So entstehen auch Benachteiligungsrisiken: Etwa kann es sein, dass ein maschinell lernendes System eine Korrelation zwischen langen Anfahrtswegen von Kandidatinnen und ihrem Kündigungsverhalten analysiert. Lehnt es in der Folge Kandidatinnen mit längeren Anfahrtswegen ab, kann dies zu Benachteiligungen bestimmter Bevölkerungsgruppen führen, die tendenziell eher außerhalb der Stadtmitte wohnen.[35]

---

[32] *Lauscher/Legner*, ZfDR 2022, 367, 372.
[33] Kapitel 3 B. (S. 35).
[34] Kapitel 3 C. (S. 36).
[35] Kapitel 8 B.II. (S. 289).

Kapitel 4

Transparenz als zentrales Element für mehr Vertrauen

Transparenz, Nachvollziehbarkeit und Erklärbarkeit sind drei Eigenschaften, die in der Debatte rund um maschinell lernende Systeme allgegenwärtig sind.[1] Die Begriffe werden nicht immer einheitlich verwendet und sind kaum voneinander zu trennen.[2] In dieser Arbeit wird Transparenz als Oberbegriff verwendet: Nachvollziehbarkeit und Erklärbarkeit führen zu Transparenz.[3]

In diesem Abschnitt wird gezeigt, was die Ursachen für Intransparenz sind, welchen Nutzen Transparenz hat und was die Mindestanforderungen sind, die für die spätere Auslegung rechtlicher Begriffe relevant sind.

Transparenz taucht in der nachfolgenden rechtlichen Analyse an verschiedenen Stellen auf: Art. 12 Abs. 1 DSGVO fordert, dass Informationen in *transparenter* und *verständlicher* Form übermittelt werden sollen.[4] Art. 5 Abs. 1 lit. a DSGVO enthält den Grundsatz, dass personenbezogene Daten auf

---

[1] *BT-Drs. 19/23700*, S. 64; *Feuerstack*, Ordnung der Wissenschaft 2022, 167; *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 19; *Müller*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 205, 219; *Waltl*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, S. 1, 1 ff.

[2] *Knobloch/Hustedt*, Der maschinelle Weg zum passenden Personal, 2019, S. 19; *Krafft/Zweig*, Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse, 2019, S. 14.

[3] Ähnlich *Rostalski*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 251, 255, die im Ergebnis ähnliche Erwägungen anstellt, Erklärbarkeit aber nicht als Unterpunkt von Transparenz sieht.

[4] Zu den Informationspflichten s. Kapitel 7 B. (S. 246).

rechtmäßige Weise, nach Treu und Glauben und einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, *Transparenz*"). Wenn eine Bewerberin oder Arbeitnehmerin wegen eines in § 1 AGG genannten Grundes eine Benachteiligung geltend macht, muss sie zumindest Indizien vorbringen, die eine Benachteiligung vermuten lassen.[5] Wenn die betroffene Person aufgrund der Intransparenz aber keine Indizien beweisen kann, ist das für sie nachteilig. Auch im KI-VO-KOM sowie im Kompromissvorschlag wird gefordert, dass der Betrieb eines Hochrisiko-KI-Systems *hinreichend transparent* ist.[6]

A. Ursachen für Intransparenz von maschinell lernenden Systemen

I. Technische und rechtliche Hürden

Die fehlende Transparenz von maschinell lernenden Systemen wird häufig unter dem Stichwort Opazität oder Blackbox-Problematik diskutiert.[7] Intransparenz betrifft sowohl die technische als auch die rechtliche Ebene.[8]

1. Technische Intransparenz

Auf technischer Ebene ist mit „*Blackbox*" gemeint, dass man nicht genau versteht, wie das maschinell lernende System zu einer Entscheidung

---

[5] Kapitel 9 B.II.1. (S. 318).

[6] Kapitel 10 B.II. (S. 355).

[7] *Europäische Kommission*, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik im Hinblick auf Sicherheit und Haftung, 2020, S. 2; *Martini*, Blackbox Algorithmus, 2018, S. 28 ff.; *Ebers*, in: Colonna/Greenstein (Hrsg.), Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence, 2022, S. 103, 107 ff.; *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 28, https://perma.cc/HST2-AGW4 (archiviert am 04.11.2023).

[8] *Tschider*, Iowa Law Review 2021, 126, 129; *Martini*, Blackbox Algorithmus, 2018, S. 33; urheber- und patentrechtliche Gründe werden nicht weiter untersucht, s. dazu etwa: *Elter*, in: Beck/Kusche/Valerius (Hrsg.), Digitalisierung, Automatisierung, KI und Recht, 2020, S. 181.

gekommen ist.[9] Je komplexer ein solches System, desto weniger ist ein Mensch in der Lage, nachzuvollziehen, wie das System funktioniert.[10] Bei neuronalen Netzen etwa ist nicht nachvollziehbar, welcher Zusammenhang genau zwischen einer Eingabe- und Ausgabeschicht besteht.[11] Aufgrund der verschiedenen neuronalen Knoten, der Gewichtung und der Kombination aus unzähligen Variablen und großen Datenmengen, die ein maschinell lernendes System verarbeitet, ist es auch für Entwicklerinnen unmöglich, die Gründe für ein Ergebnis (*Output*) eines maschinell lernenden Systems genau festzustellen.[12] Das bereits erwähnte Sprachmodell von *Microsoft* besteht aus über 530 Milliarden Parametern.[13] Ein Mensch wird kaum dazu in der Lage sein, sich überhaupt einen Überblick über diese enorme Anzahl an Parametern zu verschaffen.

2. Rechtliche Intransparenz

Rechtliche Intransparenz kann dadurch zustande kommen, dass rechtliche Vorschriften es verbieten, die Trainingsdaten eines maschinell lernenden Systems zu veröffentlichen. Handelt es sich bei Trainingsdaten um personenbezogene Daten, ist die DSGVO anwendbar.[14] Sollen personenbezogene Daten verarbeitet werden, worunter auch das Veröffentlichen von Daten fällt, muss ein datenschutzrechtlicher Erlaubnistatbestand, etwa Art. 6 Abs. 1 S. 1 DSGVO und ggf. zusätzlich

---

[9] *Bittner/Debowski/Lorenz u.a.*, NZV 2021, 505, 512; *Burrell*, Big Data & Society 3 (2016), 1-12; *Martini*, Blackbox Algorithmus, 2018, S. 28 ff.; Nachvollziehbarkeit wird auch z. T. als eigenständiger Bereich betrachtet: *Stefan Larsson/Fredrik Heintz*, Internet Policy Review 9 (2020), 6 f.

[10] *Lauscher/Legner*, ZfDR 2022, 367, 375; *Martini*, Blackbox Algorithmus, 2018, S. 194.

[11] *Buxmann/Schmidt*, Künstliche Intelligenz, 2018, S. 17; *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 16; *Rudin/Radin*, Harvard Data Science Review 1 (2019), 3.

[12] *Feuerstack*, Ordnung der Wissenschaft 2022, 167, 170.

[13] *Alvi/Kharya*, Using DeepSpeed and Megatron to Train Megatron-Turing NLG 530B, the World's Largest and Most Powerful Generative Language Model, 2021 https://perma.cc/EJ45-79G3 (archiviert am 10.01.2023).

[14] Kapitel 5 A.III.2.a)aa) (S. 65).

Art. 9 Abs. 2 DSGVO, erfüllt sein. [15] Liegen die Voraussetzungen eines Erlaubnistatbestands nicht vor, dürfen die Daten nicht veröffentlicht werden.

Außerdem können maschinell lernende Systeme als Geschäftsgeheimnis i. S. d. § 2 Nr. 1 lit. a oder c GeschGehG eingeordnet werden. [16] Geschäftsgeheimnis ist nach § 2 Nr. 1 lit. a GeschGehG eine Information, die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist. Nach § 2 Nr. 1 lit. c GeschGehG ist ein Geschäftsgeheimnis eine Information, bei der ein berechtigtes Interesse an der Geheimhaltung besteht. Üblicherweise wird ein maschinell lernendes System mit bestimmten Daten für ein Anwendungsszenario trainiert. Der genaue Trainingsprozess wird nicht öffentlich zugänglich sein – er ist also weder allgemein bekannt, noch ist er ohne Weiteres zugänglich. Mithin ist der Trainingsprozess von wirtschaftlichem Wert. Außerdem besteht im Hinblick auf Missbrauchsrisiken ggf. sogar ein berechtigtes Interesse an der Geheimhaltung. [17] Schließlich könnte es auch sein, dass es zu einer Zweckentfremdung des maschinell lernenden Systems kommt, wenn der Trainingsprozess offengelegt werden würde.

II. *Explainable AI*

Es gibt aber Modelle, die einen Blick in die *Blackbox* ermöglichen.[18] Das Forschungsfeld der *„explainable AI"* (kurz: „XAI") beschäftigt sich damit,

---

[15] *Janal*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 123.

[16] *Dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 123.

[17] Umstritten ist, ob das Merkmal des berechtigten Interesses richtlinienkonform ist. Darauf wird an dieser Stelle nicht näher eingegangen, s. dazu etwa: *dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 123, 124 ff.

[18] *Käde/Maltzan*, CR 2020, 66, 70.

dass KI erklärbar und nachvollziehbar wird.[19] Unter XAI werden bestimmte Methoden des maschinellen Lernens zusammengefasst, die eine Erklärung zu einer Entscheidung liefern, die der Mensch nachvollziehen kann.[20] Es gibt z. B. Methoden, die neuronale Netze in leichter verständliche Entscheidungsbäume umwandeln.[21] Auch wird daran geforscht, den Trainingsprozess einzelner Schichten zu untersuchen, damit man nachvollziehen kann, wie *Input-Signale* die Vorhersagen beeinflussen.[22] Für neuronale Netze und Bilddaten kann etwa die sog. *Layer-Wise Relevance Propagation* (LRP) verwendet werden.[23] Durch LRP kann man sehen, wie einzelne Eingaben das Ergebnis einer Klassifikation beeinträchtigen. Werden Bilder klassifiziert, kann man etwa herausfinden, welche Pixel in welchem Umfang das Klassifizierungsergebnis positiv oder negativ beeinflussen. Das geschieht dadurch, indem jedem *Inputwert* ein Relevanzwert zugeordnet wird.[24] Für den Menschen kann der Entscheidungsprozess auf einer sog. *Heatmap* mithilfe verschiedener Farben sichtbar gemacht werden.[25]

Eine weitere Möglichkeit sind sog. *Local Interpretable Mode-Agnostic Explanations* (*Lime*).[26] Bei *Lime* kann mithilfe eines einfacheren, oft linearen Modells ein Ergebnis eines komplizierten maschinell lernenden Systems zum

---

[19] *Bomhard/Merkle*, RDi 2021, 276, 280f.; *Konertz/Schönhof*, Das technische Phänomen "Künstliche Intelligenz" im allgemeinen Zivilrecht, 2020, S. 65; umfassend dazu s. *Barredo Arrieta/Díaz-Rodríguez/Del Ser u.a.*, Information Fusion 58 (2020), 82; *Holzinger/Goebel/Fong u. a.* (Hrsg.), xxAI - Beyond Explainable AI, 2022.

[20] *Barredo Arrieta/Díaz-Rodríguez/Del Ser u.a.*, Information Fusion 58 (2020), 82, 83; *Holzinger/Saranti/Molnar u.a.*, in: Holzinger/Goebel/Fong u.a. (Hrsg.), xxAI - Beyond Explainable AI, 2022, S. 13; *Joos/Meding*, CR 2020, 834, 838; *Krafft/Zweig*, Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse, 2019, S. 17.

[21] *Konertz/Schönhof*, Das technische Phänomen "Künstliche Intelligenz" im allgemeinen Zivilrecht, 2020, S. 65.

[22] *Ng/Soo*, Data Science – was ist das eigentlich?!, 2018, S. 144.

[23] *Holzinger/Saranti/Molnar u.a.*, in: Holzinger/Goebel/Fong u.a. (Hrsg.), xxAI - Beyond Explainable AI, 2022, S. 13, 18; *Kraus/Ganschow/Eisenträger u.a.*, Erklärbare KI, 2021, S. 29.

[24] *Kraus/Ganschow/Eisenträger u.a.*, Erklärbare KI, 2021, S. 29.

[25] *Hoeren/Niehoff*, RW 2018, 47, 59.

[26] *Dies.*, RW 2018, 47, 60; *Holzinger/Saranti/Molnar u.a.*, in: Holzinger/Goebel/Fong u.a. (Hrsg.), xxAI - Beyond Explainable AI, 2022, S. 13, 15 f.; *Kraus/Ganschow/Eisenträger u.a.*, Erklärbare KI, 2021, S. 27.

Teil nachvollzogen werden. Mithilfe des technischen Verfahrens kann so etwa erkannt werden, dass bei einer Bonitätsprüfung die Kriterien „arbeitslos", „Schulden" und „SCHUFA-Eintrag" relevant für das Ergebnis sind.[27] Zwar lassen sich mithilfe dieses Verfahrens nicht die genauen Gewichtungen des maschinell lernenden Systems erkennen. Eine betroffene Person kann so aber zumindest herausfinden, ob sachfremde Kriterien bei der Entscheidung eine Rolle gespielt haben.

Mithilfe von XAI können daher zahlreiche, bislang unerkannte Fehlergruppen enttarnt werden.[28] Eine Grenze besteht jedoch dann, wenn das Modell so komplex ist, dass auch Entwicklerinnen das Modell nicht mehr erklären können.[29] Die Methoden können dann nicht weiterhelfen, das maschinell lernende System verständlicher darzustellen.[30]

Insgesamt ist das Forschungsfeld von XAI noch nicht so weit, dass komplexe Modelle verständlich umgewandelt werden können.[31] In den nächsten Jahren wird sich in der Hinsicht noch viel entwickeln: Das Forschungsfeld von XAI wächst.[32]

B. Nutzen von Transparenz und Mindestanforderungen

Eine einheitliche Definition, wie Transparenz aus (rechtlicher) Sicht verstanden werden muss, gibt es nicht. Welches Transparenzniveau bei den

---

[27] *Hoeren/Niehoff*, RW 2018, 47, 60.

[28] *Konertz/Schönhof*, Das technische Phänomen „Künstliche Intelligenz" im allgemeinen Zivilrecht, 2020, S. 66.

[29] *Dies.*, Das technische Phänomen „Künstliche Intelligenz" im allgemeinen Zivilrecht, 2020, S. 66.

[30] *Dies.*, Das technische Phänomen „Künstliche Intelligenz" im allgemeinen Zivilrecht, 2020, S. 66.

[31] S. *Martini*, Blackbox Algorithmus, 2018, S. 194; Braegelmann/Kaulartz/*Körner*, Kap. 2.4. Rn. 27.

[32] S. etwa die Forschung des Fraunhofer Instituts zur XAI, https://perma.cc/93QX-D74L (archiviert am 16.01.2023).

jeweiligen Vorschriften gilt, wird an den jeweiligen Stellen der Arbeit geprüft.[33]

I. Transparenz als Oberbegriff für Nachvollziehbarkeit und Erklärbarkeit

Der Duden nennt als eine von drei Bedeutungen für das Wort Transparenz „Nachvollziehbarkeit". [34] Nachvollziehbarkeit ist die Folge transparenter Prozesse: Wenn man offenlegt, wie eine Entscheidung zustande gekommen ist, kann die betroffene Person diese auch nachvollziehen. Bei maschinell lernenden Systemen wird man kaum erreichen, dass die betroffenen Personen alle Schritte tatsächlich nachvollziehen. [35] Dafür müssten die Transparenzpflichten sehr weit gehen und alle denkbaren Schritte in der Entwicklung eines maschinell lernenden Systems offenlegen. Dass die betroffenen Personen umfassend den gesamten Prozess nachvollziehen, ist aber auch gar nicht notwendig: Etwa wäre es nicht förderlich, wenn der Softwarecode offengelegt werden würde. Abgesehen davon, dass er für die meisten Personen nicht aufschlussreich wäre, könnte es zu Manipulationsrisiken führen, wenn der Code offengelegt wird: So wurde nach der Veröffentlichung der Wirkweise des „*PageRank-Algorithmus*", den das Unternehmen *Google* für die Anzeige der Suchergebnisse benutzt hat, dieser Algorithmus gezielt ausgenutzt, damit Suchergebnisse weiter oben angezeigt werden.[36]

Erklärbarkeit bezieht sich hingegen im Kontext von maschinell lernenden Systemen darauf, die konkrete Entscheidung zu verstehen. [37] Für eine Einzelentscheidung müssen die wesentlichen Einflussfaktoren aufgezeigt werden können, damit sie erklärbar ist.[38]

---

[33] S. etwa: Kapitel 7 B. (S. 246);Kapitel 10 B.II. (S. 355).

[34] Duden zu „Transparenz": https://perma.cc/YK6C-TYWA (archiviert am 28.11.2022).

[35] *Krafft/Zweig*, Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse, 2019, S. 17.

[36] *Zweig*, Algorithmische Entscheidungen: Transparenz und Kontrolle, 2019, S. 8.

[37] *Sesing/Baum*, DSRITB 2019, 435, 439; vgl. *Käde/Maltzan*, CR 2020, 66, 67 f.

[38] *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen, 2018, S. 30.

II. Relevante Auslegungsaspekte

Für die Auslegung des Begriffs Transparenz im Recht muss berücksichtigt werden, dass Transparenz ein abstrakter Sammelbegriff ist, der verschiedene Komponenten beinhaltet. [39] Transparenz kann für maschinell lernende Systeme auf zwei Ebenen verstanden werden: die *materielle* und die *formelle* Ebene.[40] Die materielle Ebene umfasst, dass die Person verstehen sollte, was die wesentlichen inhaltlichen Komponenten sind, die hinter einer Entscheidung stehen. Die Entscheidung muss für die betroffene Person insofern erklärbar sein, dass sie versteht, welche Komponenten für die konkrete Entscheidung relevant geworden sind.[41] Die formelle Ebene betrifft die Funktionsweise des maschinell lernenden Systems. Die betroffene Person sollte nachvollziehen können, wie ein maschinell lernendes System grundsätzlich funktioniert, um die Risiken und Chancen gleichermaßen einordnen zu können.[42]

III. Nutzen von Transparenz

Die Enquete-Kommission KI führt in einem Bericht zum Aspekt der Transparenz aus, dass Transparenz eine unverzichtbare Grundlage sei, um Rechtsverletzungen zu identifizieren und Rechte durchzusetzen. [43] Nur wenn man das generierte Ergebnis des maschinell lernenden Systems nachvollziehen und erklären kann, ist man auch in der Lage, sich etwa gegen diskriminierende Entscheidungen eines derartigen Systems zur Wehr zu setzen.

Ein weiterer wichtiger Nutzen von Transparenz ist, dass durch Nachvollziehbarkeit und Erklärbarkeit ein Vertrauen in die Entscheidung des

---

[39] *Janal* beschreibt Transparenz als einen „schillernden" Begriff, s. *Janal*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 123.

[40] Vgl. *Knitter*, Digitale Weisungen, 2022, S. 154 f.; ähnliche inhaltliche Gedanken: *Nink*, Justiz und Algorithmen, 2021, S. 338 f.

[41] *Bittner/Debowski/Lorenz u.a.*, NZV 2021, 505, 512 f.

[42] Ähnlich auch die Definition von Transparenz nach *Manthey*: *Manthey*, Das datenschutzrechtliche Transparenzgebot, 2020, S. 42.

[43] *BT-Drs. 19/23700*, S. 84 m. V. a. Kommissionsdrucksache 19(27)45 vom 6. Mai 2019.

maschinell lernenden Systems erwächst. Vertrauen ist elementar, um Ergebnisse maschinell lernender Systeme zu akzeptieren.[44]

C. Zwischenergebnis: Zwei Bestandteile des Transparenzbegriffs

1. Die Intransparenz maschinell lernender Systeme ist sowohl auf technischer als auch rechtlicher Ebene ein Problem für das Vertrauen in derartige Systeme. Mithin ist die Intransparenz ein wesentliches Hindernis dafür, dass maschinell lernende Systeme und die von diesen generierten Entscheidungen akzeptiert werden.

2. Der Transparenzbegriff wird im wissenschaftlichen Kontext nicht einheitlich verwendet. Transparenz setzt sich nach dem Verständnis dieser Arbeit aus Nachvollziehbarkeit und Erklärbarkeit zusammen.[45] Auf materieller Ebene muss die betroffene Person nachvollziehen können, welche Kriterien die Grundlage für die Entscheidung waren (Nachvollziehbarkeit). Die konkrete Entscheidung muss für die Person verständlich sein. Auf formeller Ebene sollte die betroffene Person die grundsätzliche Funktionsweise des algorithmischen Systems, welches zur Entscheidung geführt hat oder unterstützend zur Entscheidung eingesetzt wurde, verstehen können (Erklärbarkeit).

3. Nachvollziehbarkeit bezieht sich mithin auf die konkrete Einzelfallentscheidung, die ein System generiert. Erklärbarkeit ist eine Eigenschaft des algorithmischen Systems in seiner Gesamtheit. Diese beiden Bestandteile des Transparenzbegriffs sind grundsätzlich unabhängig voneinander zu beurteilen, stehen aber in einem engen Zusammenhang. In der Regel wird eine Entscheidung nicht nachvollziehbar sein, wenn das algorithmische System nicht erklärbar ist. Es ist aber dennoch denkbar, dass ein grundsätzlich erklärbares System eine nicht nachvollziehbare Entscheidung generiert.

---

[44] Vgl. *ebd.*, S. 84; vgl. dazu auch: *Schaar*, in: Klafki/Würkert/Winter (Hrsg.), Digitalisierung und Recht, 2017, S. 29, 34; kritisch dazu s. etwa *Coester*, DuD 2020, 245.

[45] Kapitel 4 B.I. (S. 45).

Teil 1

Zusammenfassung

1. Wenn von KI gesprochen wird, sind insbesondere Methoden des maschinellen Lernens gemeint. Lernalgorithmen suchen nach Mustern in Datensätzen. Mithilfe eines zweiten „klassischen" Algorithmus kann ein System entstehen, welches ein bestimmtes Problem löst. Wie gut ein algorithmisches System ist, hängt von der Qualität der Trainingsdaten ab.[1] Derartige Systeme werden im Kontext dieser Arbeit als maschinell lernende Systeme bezeichnet. Im Gegensatz dazu können rein regelbasierte, also nicht-lernende Systeme mithilfe klassischer Algorithmen anhand eines bestimmten *Inputs* Schritt für Schritt einen jeweiligen *Output* bestimmen. [2] Der Oberbegriff „algorithmische Systeme" erfasst sowohl maschinell lernende als auch nicht-lernende Systeme.

2. Die Besonderheit eines Lernalgorithmus gegenüber einem klassischen Algorithmus besteht darin, dass er Wissen generieren kann, indem er Rückschlüsse aus Daten zieht und seine Vorgehensweise anpasst. Dadurch kann ein Lernalgorithmus auch für unbekannte Fälle eine Lösung präsentieren. Das führt allerdings dazu, dass das maschinell lernende System zu einer „*Blackbox*" wird.[3] Wird etwa ein neuronales Netz eingesetzt, kann es sogar sein, dass selbst Entwicklerinnen nicht

---

[1] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 53; *Kroll/Huey/Barocas u.a.*, Univ. Pa. Law Rev. 165 (2017), 633, 688; *Lauscher/Legner*, ZfDR 2022, 367, 371; *Neutatz/Abedjan*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 1, 4; s. dazu auch: Kapitel 8 B.I (S. 288).

[2] S. *Krüger/Lischka*, Damit Maschinen den Menschen dienen können, 2018, S. 13.

[3] Kapitel 4 A.I.1. (S. 40).

genau erklären können, wie das maschinell lernende System den *Output* bestimmt hat. Daher ist aus rechtlicher Sicht vor allem interessant, wie die Transparenzanforderungen, die sich sowohl aus der DSGVO als auch aus dem KI-VO-KOM ergeben, gewahrt werden können.

3. Bei maschinell lernenden Systemen ist Transparenz eine Herausforderung. Eine absolute Definition für Transparenz gibt es nicht. Diese Arbeit versteht den Begriff wie folgt[4]: Transparenz setzt sich aus Nachvollziehbarkeit und Erklärbarkeit zusammen. Auf materieller Ebene muss die betroffene Person nachvollziehen können, welche Kriterien die Grundlage für die Entscheidung waren. Die konkrete Entscheidung muss so für die Person verständlich sein. Auf formeller Ebene sollte die betroffene Person die grundsätzliche Funktionsweise des maschinell lernenden Systems, welches zur Entscheidung geführt hat oder unterstützend zur Entscheidung eingesetzt wurde, verstehen können.

[4] *Knitter*, Digitale Weisungen, 2022, S. 154 f.

Teil 2

Datenschutzrechtliche Anforderungen an algorithmische Systeme

Werden personenbezogene Daten mittels algorithmischer Systeme verarbeitet, müssen insbesondere die Vorgaben der DSGVO sowie im Beschäftigtendatenschutz die Vorgaben des BDSG beachtet werden. Der folgende zweite Teil gibt zunächst einen Überblick über die rechtlichen Rahmenbedingungen. [1] Sodann wird herausgearbeitet, wann eine Datenverarbeitung durch algorithmische Systeme rechtmäßig ist.[2] Schließlich werden die Betroffenenrechte und die Pflichten der Verantwortlichen erläutert.[3]

[1] Kapitel 5 (S. 53).
[2] Kapitel 6 (S. 97).
[3] Kapitel 7 (S. 241).

Kapitel 5

Überblick über die rechtlichen Rahmenbedingungen

Anwenderinnen algorithmischer Systeme müssen wissen, welche rechtlichen Vorgaben sie beachten müssen. Für den Untersuchungsgegenstand dieser Arbeit ist es daher wichtig, herauszuarbeiten, welche rechtlichen Rahmenbedingungen es gibt und in welchem Verhältnis die unterschiedlichen Vorgaben zueinanderstehen. Dabei muss man zwischen Vorgaben auf unionaler und auf nationaler Ebene trennen.

A. Unions- und völkerrechtliche Vorgaben

I. Anwendungsvorrang des Unionsrechts

Das Unionsrecht hat grundsätzlich Anwendungsvorrang vor nationalem Recht.[1] Der Vorrang ist nicht ausdrücklich geregelt, die Begründung des Vorrangs ist unterschiedlicher Art.[2] Für Verordnungen ergibt sich der Anwendungsvorrang aus Art. 288 Abs. 2 AEUV: Sie gelten unmittelbar in jedem Mitgliedsstaat. Richtlinien hingegen müssen erst von den Mitgliedstaaten umgesetzt werden (vgl. Art. 288 Abs. 3 AEUV). Unter bestimmten Voraussetzungen können Richtlinien auch ohne nationalen Umsetzungsakt unmittelbar wirken und Unionsbürgerinnen begünstigen.[3]

---

[1] BVerfG, 1.12.2020 – 2 BvR 1845/18, 2 BvR 2100/18, NJW 2021, 1518, 1523 Rn. 58; EuGH, 22.10.1998 – C-10/97 bis C-22/97, *Ministero delle Finanze ./. IN.CO.GE.'90 Srl u. a.*, NJW 1999, 200, 202 Rn. 20; EUV/AEUV/*Streinz*, Art. 4 EUV Rn. 35.

[2] Calliess/Ruffert/*Ruffert*, Art. 1 AEUV Rn. 17.

[3] EuGH, 19.1.1982 – Rs 8/81, NJW 1982, 499; EUV/AEUV/*Streinz*, Art. 4 EUV Rn. 40.

Das ist aber für den Untersuchungsgegenstand der Arbeit nicht relevant, sodass darauf nicht weiter eingegangen wird.

Sowohl die DSGVO als auch die zukünftig geltende KI-Verordnung gelten mithin unmittelbar in den Mitgliedstaaten, ohne dass sie umgesetzt werden müssen. Die DSGVO schützt insbesondere das Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO) und ist damit eine Verordnung, die „ein Grundrecht und dessen Durchsetzung ausführlich regelt“[4]. Mit den beiden Beschlüssen zum „Recht auf Vergessen I und II“[5] hat der Erste Senat des BVerfG sich zum Verhältnis von Unions- und Verfassungsrecht geäußert. Ist der Anwendungsbereich des Unionsrechts eröffnet, greift er auf die Grundrechte der GRCh zurück. Ist das innerstaatliche Recht nicht vollständig durch Unionsrecht determiniert, dienen die nationalen Grundrechte als Prüfungsmaßstab. [6] Im Anwendungsbereich der DSGVO führen die Mitgliedstaaten grundsätzlich Unionsrecht durch und sind an die unionalen Grundrechte gebunden.[7]

II. Zusammenspiel von Art. 8 EMRK, Art. 16 AEUV, Art. 7 und 8 GRCh

Maßgebliches Unionsgrundrecht ist vor allem Art. 8 GRCh[8], der den Schutz personenbezogener Daten regelt. Bedeutung hat aber auch Art. 7 GRCh, der das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation einer Person sicherstellt.

---

[4] Gola/Heckmann/*Pötters*, Art. 1 DSGVO Rn. 7.

[5] BVerfG, 6.11.2019 – 1 BvR 16/13, NJW 2020, 300; BVerfG, 6.11.2019 – 1 BvR 276/17, NJW 2020, 314.

[6] BVerfG, 6.11.2019 – 1 BvR 16/13, NJW 2020, 300, 301 Rn. 42; *Kühling*, NJW 2020, 275, 279.

[7] *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, A. II. 3. Rn. 193.

[8] Die Grundrechtecharta der Europäischen Union trat am 1. Dezember 2009 mit dem Vertrag von Lissabon in Kraft, vgl. Abl. Nr. C 306/1.

1. Verhältnis von Art. 8 EMRK, Art. 16 AEUV, Art. 7 und 8 GRCh

Im Jahr 1987 entwickelte der EGMR aus Art. 8 EMRK [9] das erste Datenschutzgrundrecht.[10] Art. 8 EMRK war bereits in der ersten Fassung der EMRK von 1950 vorhanden.[11] Zwar schützt der Wortlaut nicht ausdrücklich die personenbezogenen Daten, sondern das Recht auf Achtung des Privat- und Familienlebens. Zentraler Teilbereich der Privatsphäre ist jedoch der Schutz personenbezogener Daten.[12] Der Schutzbereich wird grundsätzlich weit ausgelegt: Jede Erhebung, Speicherung, Weitergabe oder sonstige Verarbeitung personenbezogener Daten oder menschlicher Kommunikation ist als Eingriff in Art. 8 EMRK zu werten.[13]

Die erste Fassung der EU-Grundrechtecharta aus dem Jahr 2000 enthielt mit Art. 8 GRCh ein eigenes Recht auf Schutz personenbezogener Daten, das über Art. 6 Abs. 1 EUV primärrechtlichen Geltungsanspruch erhalten hat.[14] Art. 8 GRCh steht in engem Zusammenhang mit Art. 7 GRCh[15], welcher das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation schützt. Art. 7 GRCh ist fast wortgleich mit Art. 8 EMRK. Der EuGH verwendet Art. 7 und 8 GRCh häufig zusammen: Die Achtung des Privatlebens erstreckt sich „hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information, die eine bestimmte oder bestimmbare natürliche Person betrifft“[16].

---

[9] Die Europäische Menschenrechtskonvention (EMRK) wurde am 4. November 1950 unterzeichnet und ist am 3. September 1953 in Kraft getreten; vgl. BGBl. 1954 II S. 14.

[10] EGMR, 26.3.1987 – 9248/81, *Torsten Leander ./. Schweden*, EGMR-E 3, 430.

[11] Convention for the protection of human rights and fundamental freedom, 4.11.1950, SEV Nr. 005.

[12] Vgl. EGMR, 24.1.2019 – 43514/15, *Catt ./. Vereinigtes Königreich*, NVwZ 2020, 377.

[13] *Leeb/Liebhaber*, JuS 2018, 534, 535.

[14] BeckOK Datenschutzrecht/*Schneider*, Syst. B. Völker- und unionsverfassungsrechtliche Grundlagen C. III. Rn. 22.

[15] EuGH, 9.11.2010 – C-92/09, *Volker und Markus Schecke GbR (C-92/09) und Hartmut Eifert (C-93/09) ./. Land Hessen,* Rn. 47.

[16] EuGH, 9.11.2010 – C-92/09, *Volker und Markus Schecke GbR (C-92/09) und Hartmut Eifert (C-93/09) ./. Land Hessen,* Rn. 52; a. A.: *Kühling/Raab*, die Art. 8 GRCh als *lex specialis* gegenüber Art. 7 GRCh einordnen: Kühling/Buchner/*Kühling/Raab*, A. B. II. 3 b) Rn. 26.

a) EMRK als Rechtserkenntnisquelle

Art. 6 Abs. 3 EUV normiert, dass die Grundrechte der EMRK als allgemeine Grundsätze Teil des Unionsrechts sind. Nach Art. 52 Abs. 3 GRCh gilt, dass, „soweit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, [...] sie die gleiche Bedeutung und Tragweite [haben], wie sie ihnen in der genannten Konvention verliehen wird". Dadurch soll die Kohärenz zwischen GRCh und EMRK sichergestellt werden: Die EMRK wird zum mittelbaren Bestandteil des Unionsrechts.[17] Bis die Union der EMRK beigetreten ist (Art. 6 Abs. 2 S. 1 EUV), ist die EMRK nicht unmittelbarer Bestandteil des Unionsrechts, sondern Rechtserkenntnisquelle.[18] Auch wenn die Union nach Art. 6 Abs. 2 S. 1 EUV rechtlich verpflichtet ist der EMRK beizutreten, ist es aktuell nicht absehbar, dass die Union ihrer Verpflichtung zum Beitritt nachkommen wird.[19] Der EuGH hat mit seinem Gutachten 2/13[20] vom 18.12.2014 das Beitrittsabkommen für unionsrechtswidrig erklärt. Hauptkritikpunkt des EuGH war, dass ein Beitritt zur EMRK womöglich die Autonomie des Unionsrechts untergraben könne, etwa weil es keine Norm gebe, die die Zuständigkeit des EGMR nach Art. 33 EMRK für Rechtsstreitigkeiten zwischen den Mitgliedstaaten ausschließe.[21] Die Europäische Kommission hat aber angekündigt, dass sie sich um die Wiederaufnahme der Beitrittsverhandlungen bemühen möchte.[22]

Momentan bleibt es somit dabei, dass die EMRK bloße Rechtserkenntnisquelle ist. Das bedeutet, dass die GRCh mit Rücksicht auf die EMRK auszulegen ist und auch nicht hinter ihr zurückbleiben darf: Die

---

[17] EuArbRK/*Schubert*, Art. 52 GRC Rn. 10.

[18] Calliess/Ruffert/*Kingreen*, Art. 6 EUV Rn. 7; NK-GRC/*Schwerdtfeger*, Art. 52 GRC Rn. 52.

[19] Calliess/Ruffert/*Kingreen*, Art. 6 EUV Rn. 33.

[20] EuGH, Gutachten 2/13, ECLI:EU:C:2014:2454.

[21] EuGH, Gutachten 2/13, ECLI:EU:C:2014:2454 Rn. 201 ff.; Calliess/Ruffert/*Kingreen*, Art. 6 EUV Rn. 31.

[22] Europäische Kommission, Die Stärkung der Rechtsstaatlichkeit in der Union. Ein Konzept für das weitere Vorgehen, COM(2019) 343 final, 9; Calliess/Ruffert/*Kingreen*, Art. 6 EUV Rn. 33.

EMRK ist unionsrechtlicher Mindeststandard des Grundrechtsschutzes.[23] Das geht auch aus Art. 53 GRCh hervor: Gem. Art. 53 GRCh darf das Schutzniveau der EMRK nicht durch die Charta unterlaufen werden. Der Union ist es aber möglich, einen weitergehenden Schutz zu gewähren (vgl. Art. 52 Abs. 3 S. 2 GRCh). Auf nationaler Ebene gilt, dass die Grundrechte des GG im Lichte der EMRK ausgelegt werden: Die EMRK wird als Auslegungshilfe herangezogen.[24]

Art. 16 Abs. 1 AEUV[25] wiederholt den Wortlaut des Art. 8 GRCh. Diskutiert wird, wie es sich auf die Schranken des Grundrechts auswirkt, dass es in Art. 16 AEUV erneut erwähnt wird.[26] Art. 16 AEUV selbst enthält – anders als Art. 8 GRCh – keine normierten Schranken. Aufgrund von Art. 52 GRCh, der festlegt, dass die Ausübung der durch die Charta anerkannten Rechte im Rahmen der in den Verträgen festgelegten Bedingungen und Grenzen erfolgt, könnte man schlussfolgern, dass das Datenschutzgrundrecht schrankenlos gewährleistet sei.[27] Die Schranken der Art. 8 Abs. 2 GRCh und Art. 52 Abs. 2 GRCh würden leerlaufen. Teilweise wird daher vertreten, Art. 52 Abs. 2 GRCh nicht anzuwenden [28] oder für die nähere Ausgestaltung des Grundrechts auf die GRCh zurückzugreifen.[29] Letzteres ist eine dogmatische Frage, die nicht weiter vertieft werden soll. Entscheidend ist: Die Schranken in Art. 52 Abs. 1 GRCh und Art. 8 Abs. 2 GRCh sind relevant für die Grundrechtsprüfung und müssen berücksichtigt werden. Nach Art. 8 Abs. 2 GRCh dürfen die Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen

---

[23] EuArbRK/*Schubert*, Art. 6 EUV Rn. 64.

[24] BVerfG, 6.11.2019 – 1 BvR 16/13, NJW 2020, 300, 303 Rn. 58.

[25] Der Vertrag über die Arbeitsweise der Europäischen Union (AEUV), der seit Inkrafttreten des Vertrags von Lissabon gemeinsam mit dem EUV die maßgebliche Grundlage für die Europäische Union ist; konsolidierte Fassung in der Bekanntmachung vom 9.5.2008 vgl. ABl. EG Nr. C 115.

[26] BeckOK Datenschutzrecht/*Schneider*, Syst. B. Völker- und unionsverfassungsrechtliche Grundlagen C. III. 3. Rn. 30; EUV/AEUV/*Schröder*, Art. 16 AEUV Rn. 5.

[27] EUV/AEUV/*Schröder*, Art. 16 AEUV Rn. 5.

[28] Vgl. NK-GRC/*Bernsdorff*, Art. 8 GRCh Rn. 24; Calliess/Ruffert/*Kingreen*, Art. 16 AEUV Rn. 4.

[29] Geiger/Khan/Kotzur/*Kotzur*, Art. 16 AEUV Rn. 2.

gesetzlich geregelten legitimen Grundlage verarbeitet werden. Auf einfachgesetzlicher Ebene sind diese Grundprinzipien in der DSGVO verankert.[30] Der EuGH hat selbst stets nur auf Art. 7, 8 GRCh Bezug genommen und Art. 16 Abs. 1 AEUV nicht als Prüfungsmaßstab herangezogen.[31] Art. 16 Abs. 1 AEUV kommt mithin keine eigenständige Bedeutung zu.[32] Vielmehr soll die Wiederholung des Datenschutzgrundrechts die besondere Bedeutung für das gesamte Unionsrecht betonen.[33]

b) Grundrechtsbindung Privater

Grundsätzlich binden Art. 7, 8 GRCh gem. Art. 51 Abs. 1 S. 1 GRCh die Organe, Einrichtungen und sonstige Stellen der Union sowie die Mitgliedstaaten, soweit letztere Unionsrecht durchführen. Private sind mithin nicht unmittelbar an Art. 7, 8 GRCh gebunden.[34] Das Datenschutzgrundrecht wird aber nicht nur von staatlicher Seite gefährdet. Vielmehr sind viele Arbeitnehmerinnen bei privaten Arbeitgeberinnen beschäftigt, die Beschäftigtendaten verarbeiten.[35] Auch im Falle solcher privatrechtlich geführter Unternehmen kann das Datenschutzgrundrecht gefährdet werden.

Vor diesem Hintergrund ist die Entscheidung des EuGH v. 24.9.2019 zu berücksichtigen, die noch zur DSRL erging.[36] In dieser Entscheidung hat der EuGH entschieden, dass ein Suchmaschinenbetreiber Sorge dafür tragen müsse, dass die Tätigkeit der Suchmaschine den Anforderungen der DSRL entspreche.[37] Nur so könnten die Art. 7, 8 GRCh gewahrt werden, deren

---

[30] S. dazu die Ausführungen unter: Kapitel 6 (S. 97).

[31] EuGH, 8.4.2014 – C-293/12, C-594/12, *Digital Rights Ireland Ltd ./. Minister for Communications, Marine and Natural Resources u. a.*, NJW 2014, 2169.

[32] Kühling/Buchner/*Kühling/Raab*, A. B. II. 3. c) Rn. 35.

[33] EUV/AEUV/*Schröder*, Art. 16 AEUV Rn. 6.

[34] *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 2 III. 5. Rn. 62; *Streinz/Michl*, EuZW 2011, 384, 385.

[35] *Streinz/Michl*, EuZW 2011, 384, 385.

[36] EuGH, 24.9.2019 – C-136/17, *GC u. a. ./. Commission nationale de l'informatique et des libertés (CNIL)*, ZD 2020, 36.

[37] EuGH, 24.9.2019 – C-136/17, *GC u. a. ./. Commission nationale de l'informatique et des libertés (CNIL)*, ZD 2020, 36, 37.

Schutz durch die Vorschriften der DSRL bezweckt sei.[38] Diese Rechtsprechung hat der EuGH mit Blick auf die DSGVO fortgeführt.[39]

Der EuGH ordnet jedoch nicht dogmatisch ein, auf welche Weise die Grundrechte zwischen Privaten wirken.[40] Er benutzt insbesondere nicht den Begriff der „mittelbare Drittwirkung“[41]. Das Konzept der mittelbaren Drittwirkung bezeichnet nach dem BVerfG, dass die Grundrechte in privatrechtliche Rechtsbeziehungen ausstrahlen.[42] Von den Fachgerichten sind sie vor allem über zivilrechtliche Generalklauseln und unbestimmte Rechtsbegriffe zu berücksichtigen, wenn das Fachrecht in Privatrechtsverhältnissen ausgelegt wird.[43] Einige Stimmen in der Literatur wollen dieses Konzept der mittelbaren Drittwirkung auf das Unionsrecht übertragen.[44] BGH und BVerfG teilen diese Auffassung indes nicht.[45] Dem ist insofern zuzustimmen, als nationale Grundsätze auf unionsrechtlicher Ebene unbedeutend sind. Im Ergebnis herrscht aber zurecht Einigkeit, dass die Grundrechte der GRCh in einer Weise zwischen Privaten wirken, die der mittelbaren Drittwirkung im Sinne des deutschen Rechts ähnelt.[46]

---

[38] *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 2 III. 5. Rn. 64 m.w.N.; EuGH, 24.9.2019 – C-136/17, *GC u. a. ./. Commission nationale de l'informatique et des libertés (CNIL)*, ZD 2020, 36.

[39] EuGH, 8.12.2022 – C-460/20, *TU, RE ./. Google LLC*, EuZW 2023, 139.

[40] S. dazu: Jarass/Pieroth/*Jarass*, Art. 51 GRCh Rn. 36.

[41] BVerfG, 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667, 1668 Rn. 32.

[42] BVerfG, 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667, 1668 Rn. 32.

[43] BVerfG, 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667, 1668 Rn. 32.

[44] *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 2 Rn. 64; Jarass/Pieroth/*Jarass*, Art. 51 GRCh Rn. 38 ff.

[45] BVerfG, 6.11.2019 – 1 BvR 276/17, NJW 2020, 314, 322 Rn. 97; BGH, 3.5.2022 – VI ZR 832/20, NJW 2022, 2476, 2478 Rn. 18.

[46] BVerfG, 6.11.2019 – 1 BvR 276/17, NJW 2020, 314, 322 Rn. 97; BGH, 3.5.2022 – VI ZR 832/20, NJW 2022, 2476, 2478 Rn. 18; Dörr/Grote/Marauhn/*Krieger*, Kap. 6 Rn. 92; *Petri*, EuZW 2023, 139, 147.

Es gibt aber auch Entscheidungen des EuGH[47], die sogar auf eine unmittelbare Drittwirkung hindeuten.[48] Das soll an dieser Stelle nicht weiter vertieft werden. Vielmehr bleibt Folgendes festzuhalten: Auch wenn bislang nicht eindeutig geklärt ist, wie es dogmatisch einzuordnen ist[49], dass die Grundrechte der GRCh auch im Privatrechtsverhältnis wirken, steht fest, dass sie im Privatrechtsverhältnis berücksichtigt werden müssen, wenn Vorschriften der DSGVO ausgelegt werden.[50]

2. Art. 7, 8 GRCh als maßgebliches Datenschutzgrundrecht

Art. 7, 8 GRCh werden für das Grundrecht auf Datenschutz herangezogen. Art. 16 AEUV kommt keine eigenständige Bedeutung zu. Die EMRK und die zu Art. 8 EMRK aufgeführten Grundsätze sind bei der Auslegung entsprechend zu berücksichtigen. Das Schutzniveau der EMRK darf nicht unterschritten werden. Wird die Rechtfertigung geprüft, sind die Schranken des Art. 52 Abs. 1 GRCh und Art. 8 Abs. 2 GRCh maßgeblich. Art. 7, 8 GRCh sind auch im Privatrechtsverhältnis zu berücksichtigen, wenn Vorschriften der DSGVO ausgelegt werden.

3. Schutzbereich von Art. 7, 8 GRCh

a) Sachlicher Schutzbereich

Der sachliche Schutzbereich des Datenschutzgrundrechts umfasst personenbezogene Daten, d. h. alle Informationen über eine bestimmte oder bestimmbare Person.[51] Zum geschützten Verhalten gehört, über die Verwendung der eigenen Daten zu entscheiden und damit insbesondere das

---

[47] EuGH, C-569/16 und C-570/16, *Stadt Wuppertal ./. Maria Elisabeth Bauer (C-569/16), Volker Willmeroth als Inhaber der TWI Technische Wartung und Instandsetzung Volker Willmeroth eK ./. Martina Broßonn (C570/16)*, NZA 2018, 1467.

[48] S. dazu: Dörr/Grote/Marauhn/*Krieger*, Kap. 6 Rn. 92.

[49] *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 2 Rn. 64; Dörr/Grote/Marauhn/*Krieger*, Kap. 6 Rn. 92 ff.

[50] *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 2 Rn. 64; umfassend dazu: *Fischer*, Die Horizontalwirkung der EU-Grundrechtecharta im Arbeitsrecht, 2023, S. 230 ff.

[51] Kühling/Buchner/*Kühling/Raab*, A. B. II. 3 b) Rn. 27.

Recht, dass Dritte keine personenbezogenen Daten erheben oder verwenden und ggf. unrichtige oder nicht mehr benötigte Daten löschen.[52]

b) Persönlicher Schutzbereich

Der persönliche Schutzbereich erstreckt sich auf natürliche Personen und juristische Personen.[53] Der EuGH ist der Auffassung, dass juristische Personen sich auf das Grundrecht berufen können, wenn der Name der juristischen Person eine oder mehrere natürliche Personen bestimme.[54] Er begründet diese Auffassung nicht weiter. In dem zu entscheidenden Fall bestimmte der Name der GbR unmittelbar natürliche Personen, sodass sich die GbR auf den Schutz durch Art. 7, 8 GRCh berufen konnte.

Es kann aber für den Grundrechtsschutz nicht entscheidend sein, ob der Name eine natürliche Person bestimmt.[55] Entscheidend muss sein, ob ein persönlichkeitsrelevanter Schutz notwendig ist.[56] Das ist der Fall, wenn Daten über juristische Personen zugleich Aussagen über natürliche Personen enthalten.[57] Das ist etwa bei einer Ein-Mann-GmbH, unabhängig von deren Namen, oder eben dann der Fall, wenn schon der Name einer juristischen Person auf eine natürliche Person verweist.[58]

III. DSGVO als maßgebliche Verordnung für den Schutz personenbezogener Daten

Die DSGVO gilt seit dem 25. Mai 2018. Sie dient gem. Art. 1 Abs. 1 DSGVO dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Art. 1 Abs. 2 DSGVO sieht vor, dass die Verordnung die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten sichert. Die

---

[52] Calliess/Ruffert/*Kingreen*, Art. 8 GRCh Rn. 10.

[53] Kühling/Buchner/*Kühling/Raab*, A. B. II. 3. b) Rn. 27.

[54] EuGH, 9.11.2010 – C-92/09, *Volker und Markus Schecke GbR (C-92/09) und Hartmut Eifert (C-93/09) ./. Land Hessen,* Rn. 53.

[55] Calliess/Ruffert/*Kingreen*, Art. 8 GRCh Rn. 12.

[56] Kühling/Buchner/*Kühling/Raab*, A. B II. 3. b) Rn. 27.

[57] Kühling/Buchner/*dies.*, A. B. II. 3. b).

[58] Kühling/Buchner/*dies.*, A. B. II. 3 b) Rn. 27.

DSGVO konkretisiert den Schutz durch das europäische Primärrecht, d. h. insbesondere den durch Art. 7, 8 GRCh vorgesehenen Schutz personenbezogener Daten.[59]

1. Auslegung der DSGVO

Die DSGVO ist im Lichte der Unionsgrundrechte und Grundfreiheiten auszulegen.[60] Die Grundrechte und Grundfreiheiten werden im Rahmen der Abwägung bei den Erlaubnistatbeständen der Art. 6 und 9 DSGVO maßgeblich berücksichtigt.[61]

Außerdem können die Erwägungsgründe Hinweise auf den Zweck der Vorschriften der DSGVO enthalten.[62] Sie sind Teil des Rechtsakts und geben Aufschluss über die Ziele und Hintergründe.[63] Die Erwägungsgründe sind aber nicht rechtlich verbindlich. [64] Insbesondere ist der Wortlaut der Erwägungsgründe nicht gleichermaßen verbindlich wie der Wortlaut der konkreten Vorschrift in der Verordnung.

Für die Auslegung der DSGVO sind zudem die Stellungnahmen und Leitlinien der Art. 29-Datenschutzgruppe, des EDSA und die Kurzpapiere der DSK zu berücksichtigen:

---

[59] Gola/Heckmann/*Pötters*, Art. 1 DSGVO Rn. 7; zur Grundrechtsbindung Privater s. Kapitel 5 A.II.1.b) (S. 58).

[60] Noch zur Vorgängerrichtlinie 95/46/EG (Abl. L 281 vom 23.11.1995) s. EuGH, 1.10.2015 – C-230/14, *Weltimmo ./. Nemzeti Adatvédelmi és Információszabadság Hatóság*, NJW 2015, 3636, 3638 Rn. 25; EuGH, 13.5.2014 – C-131/12, *Google Spain SL und Google Inc. ./. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*, NJW 2014, 2257, 2260 Rn. 53; vgl. Gola/Heckmann/*Pötters*, Art. 1 DSGVO Rn. 18 m.w.N.; s. Kapitel 5 A.II.1.b) (S. 58).

[61] Gola/Heckmann/*Pötters*, Art. 1 DSGVO Rn. 20; Taeger/Gabel/*Schmidt*, Art. 1 DSGVO Rn. 19.

[62] Von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht/*Gaitanides*, Art. 19 EUV Rn. 45

[63] Von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht/*dies.*, Art. 19 EUV Rn. 45; *Wachter/Mittelstadt/Floridi*, International Data Privacy Law 2017, 76, 85.

[64] *Wachter/Mittelstadt/Floridi*, International Data Privacy Law 2017, 76, 85.

a) Art. 29-Datenschutzgruppe

Die Art. 29-Datenschutzgruppe war ein unabhängiges Beratungsgremium der Europäischen Kommission in allen Fragen im Zusammenhang mit der Richtlinie 95/46/EG,[65] der Vorgängerrichtlinie zur heute gültigen DSGVO. Sie wurde aufgrund von Art. 29 DSRL eingesetzt und hatte nur eine beratende Funktion. Die Art. 29-Datenschutzgruppe konnte keine rechtsverbindlichen Entscheidungen treffen, da die DSRL dafür keine Rechtsgrundlagen vorsah.[66]

b) Europäischer Datenschutzausschuss

Die frühere Art. 29-Datenschutzgruppe wurde durch den nach Art. 68 DSGVO gebildeten Europäischen Datenschutzausschuss (EDSA) abgelöst, als die DSGVO am 25.5.2018 gültig geworden ist.[67] Der EDSA setzt sich gem. Art. 68 Abs. 3 DSGVO aus der Leiterin einer Aufsichtsbehörde jedes Mitgliedstaats und der Europäischen Datenschutzbeauftragten oder ihrer jeweiligen Vertreterin zusammen. Anders als die Art. 29-Datenschutzgruppe kann der EDSA in den in Art. 65 Abs. 1 DSGVO aufgelisteten Fällen einen verbindlichen Beschluss erlassen. Das sind Fälle, bei denen es zu Streitigkeiten zwischen den Aufsichtsbehörden kommt. Er kann aber keinen verbindlichen Beschluss erlassen, wenn es etwa um Uneinigkeiten bei der rechtlichen Auslegung der Vorschriften der DSGVO geht. Darüber entscheidet gem. Art. 267 Abs. 1 lit. a AEUV der EuGH. Im Übrigen sind die Leitlinien und Stellungnahmen des EDSA nicht rechtsverbindlich (Art. 70 DSGVO).

Zu den Aufgaben des EDSA, die in Art. 70 DSGVO aufgeführt sind, gehört auch, eine einheitliche Rechtsanwendung der DSGVO durch Leitlinien, Empfehlungen und bewährte Verfahren zu gewährleisten. Diese Dokumente sind zwar – wie bereits erwähnt – nicht rechtlich verbindlich. Die DSGVO regelt nicht ausdrücklich, welche Durchsetzungsmechanismen verfügbar sind, wenn sich einzelne Aufsichtsbehörden nicht an die Dokumente halten.[68] Sinnvoll ist es aber, dass Behörden und Verantwortliche sich grundsätzlich an die Vorgaben des EDSA halten. Wenn eine einzelne Aufsichtsbehörde von

---

[65] Richtlinie 95/46/EG (Abl. L 281 vom 23.11.1995).
[66] Sydow/Marsch/*Schöndorf-Haubold*, Art. 65 DSGVO Rn. 4.
[67] S. https://perma.cc/YB9S-8LCX (archiviert am 14.05.2023).
[68] Kühling/Buchner/*Dix*, Art. 70 DSGVO Rn. 10.

einer Leitlinie, einer Empfehlung oder einem bewährten Verfahren abweicht, handelt es sich häufig um eine „Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat" i. S. d. Art. 64 Abs. 2 DSGVO.[69] Das wiederum erfordert eine Prüfung durch den EDSA nach Art. 64 Abs. 3 DSGVO und kann letztlich zu einem verbindlichen Beschluss gem. Art. 65 Abs. 1 lit. c DSGVO führen.[70] Behörden müssen daher trotz mangelnder Rechtsverbindlichkeit die Vorgaben des EDSA bei der Auslegung der DSGVO umsetzen.[71] Verantwortliche und Auftragsverarbeiterinnen sollten die Vorgaben beachten, weil der Verarbeitungsvorgang, der in Einklang mit der DSGVO stehen muss, von den Behörden überprüft wird.[72] Die Behörden müssen die Vorgaben des EDSA beachten. Gerichte können hingegen vom EDSA abweichende Entscheidungen hinsichtlich der Auslegung der DSGVO treffen.

In seiner konstituierenden Sitzung am 25. Mai 2018 hat der Ausschuss die von der bisherigen Art. 29-Datenschutzgruppe erlassenen Leitlinien übernommen.[73] Die Leitlinien der Art. 29-Datenschutzgruppe sind also weiterhin gültig und können ebenfalls bei der Auslegung der DSGVO herangezogen werden.

c) Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) ist ein Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie besteht aus der Bundesbeauftragten für den Datenschutz, der Landesbeauftragen für den Datenschutz und der Präsidentin des Bayerischen Landesamts für Datenschutzaufsicht.[74] Die DSK soll den Datenschutz

---

[69] Kühling/Buchner/*ders.*, Art. 70 DSGVO Rn. 10.

[70] Kühling/Buchner/*ders.*, Art. 70 DSGVO Rn. 10; Taeger/Gabel/*Hellmich*, Art. 70 DSGVO Rn. 13.

[71] Vgl. Kühling/Buchner/*Dix*, Art. 70 DSGVO Rn. 10; Taeger/Gabel/*Hellmich*, Art. 70 DSGVO Rn. 10; kritisch zur demokratischen Legitimation s. Taeger/Gabel/*dies.*, Art. 68 DSGVO Rn. 2.

[72] Vgl. Taeger/Gabel/*Hellmich*, Art. 70 DSGVO Rn. 10; *Bussche*, ZD 2021, 154, 160.

[73] S. Endorsement 1/2018, https://perma.cc/Z96Y-V4V9 (archiviert am 02.08.2022).

[74] Geschäftsordnung der DSK, Stand 21.09.2022, https://perma.cc/9BMA-PC4R (archiviert am 02.02.2023).

fördern und sich auf gemeinsame Positionen der Datenschutzaufsichtsbehörden des Bundes und der Länder verständigen. Sie erlässt deshalb Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen. Außerdem veröffentlicht die DSK Auslegungshilfen zur DSGVO. In diesen Kurzpapieren werden die von den deutschen Aufsichtsbehörden abgestimmten einheitlichen Sichtweisen zu verschiedenen Kernthemen der DSGVO wiedergegeben.[75] Die Auslegungshilfen sind ebenfalls nicht rechtlich verbindlich, werden aber wie die Stellungnahmen, Leitlinien und bewährten Verfahren der EDSA zur Auslegung der DSGVO herangezogen. Wer Daten verarbeitet und von den Vorgaben der DSGVO, die auch durch die DSK konkretisiert werden, abweicht, muss damit rechnen, dass die zuständige Aufsichtsbehörde die Datenverarbeitung für rechtswidrig hält. Ein Gericht muss aber nicht der von der DSK vertretenen Auffassung folgen.

2. Anwendungsbereich der DSGVO

Damit die DSGVO anwendbar ist, muss der Anwendungsbereich in sachlicher, persönlicher und räumlicher Hinsicht gem. Art. 1, 2 und 3 DSGVO eröffnet sein.

a) Sachlicher Anwendungsbereich

Sachlich ist die DSGVO anwendbar, wenn personenbezogene Daten ganz, teilweise oder nicht automatisiert verarbeitet werden.

aa) Personenbezogene Daten

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen („betroffene Person“). Betroffene Person kann nur eine natürliche Person von ihrer Geburt bis zu ihrem Tod sein.[76]

---

[75] S. https://perma.cc/B47G-AM97 (14.05.2023).

[76] Erwägungsgrund 27 DSGVO; Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 4.

Auf nationaler Ebene sind Daten verstorbener Personen nicht schutzlos.[77] Die Menschenwürde wirkt als postmortales Persönlichkeitsrecht nach dem Tod einer Person fort und schützt „den allgemeinen Achtungsanspruch", d. h., der Verstorbene wird „insbesondere davor bewahrt, herabgewürdigt oder erniedrigt zu werden"[78]. Das gilt aber nur auf nationaler Ebene. Die DSGVO trifft keine Regelungen dazu, wie mit personenbezogenen Daten Verstorbener umzugehen ist. Gleichwohl ergibt sich aus Erwägungsgrund 27 S. 2 DSGVO, dass abweichende Regelungen getroffen werden können. Erwägungsgründe sind nicht verbindlich[79], sind aber eine wichtige Auslegungsquelle.[80] Sie werden akzessorisch zum Normtext veröffentlicht. Damit sind sie zwar nicht dem Gesetzestext gleichzustellen, aber für die Auslegung sind sie gewichtiger als Gesetzesmaterialien.[81] Auf nationaler Ebene existiert mit dem postmortalen Persönlichkeitsrecht ein Schutz für die Daten verstorbener Personen. Der Schutz ist insofern weitergehender als auf unionaler Ebene.

(1) Informationen

Eine Information umfasst sowohl Aussagen zu überprüfbaren Eigenschaften oder tatsächlichen Verhältnissen einer Person als auch Einschätzungen und Werturteile über eine Person.[82] Der Begriff der personenbezogenen Daten wird weit gefasst.[83]

Die Art der Information ist nicht entscheidend: Freie und ungeschützte Daten gibt es nicht.[84] Besondere Kategorien personenbezogener Daten sind jedoch gem. Art. 9 DSGVO noch stärker geschützt.[85]

---

[77] Taeger/Gabel/*Schmidt*, Art. 1 DSGVO Rn. 16.

[78] BGH, 29.11.2021 – VI ZR 248/18, NJW 2022, 847, 854 Rn. 20 m.w.N.

[79] Calliess/Ruffert/*Wegener*, Art. 19 EUV Rn. 32; vgl. BeckOK Datenschutzrecht/*Worms*, Art. 17 DSGVO Rn. 9.

[80] Calliess/Ruffert/*Wegener*, Art. 19 EUV Rn. 32; *Gumpp*, ZfPW 2022, 446, 473; *Knitter*, Digitale Weisungen, 2022, S. 110 m. W. n.

[81] S. dazu ausführlich: *Gumpp*, ZfPW 2022, 446.

[82] Ehmann/Selmayr/*Klabunde*, Art. 4 DSGVO Rn. 9.

[83] *Art. 29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (WP 136), S. 7.

[84] Gola/Heckmann/*Gola*, Art. 4 DSGVO Rn. 6.

[85] Kapitel 6 A.II.1.b) (S. 105).

Bei algorithmischen Systemen zur Personalauswahl im Bewerbungsstadium oder bestehenden Arbeitsverhältnis wird das Ergebnis des Systems häufig ein Prognose- oder Planungsdatum sein. Dabei handelt es sich um Angaben über i. d. R. in der Zukunft liegende Verhältnisse einer Bewerberin oder Arbeitnehmerin.[86] Die Prognose- oder Planungsdaten werden häufig in *Score*-Werten ausgedrückt:[87] Das System berechnet z. B. den „Score" einer Person, der ausdrückt, wie hoch das Kündigungsrisiko ist.[88] Die Entscheidung über die Zukunft der Arbeitnehmerin leitet die Arbeitgeberin aus den vergangenheitsbezogenen Leistungsdaten oder dem errechneten Score ab.[89]

Es ist mithin relevant, inwiefern Prognose- und Planungsdaten als personenbezogene Daten vom Anwendungsbereich der DSGVO erfasst sind. Die Daten sind zukunftsbezogen, weshalb man anzweifeln könnte, dass die Daten bereits zur Identität der Person i. S. d. Art. 4 Nr. 1 DSGVO gehören.[90] Die Art. 29-Datenschutzgruppe[91] ist der Auffassung, dass Daten sich auch auf eine Person beziehen, „wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird"[92]. Dieser Auffassung ist zuzustimmen. Wenn die Daten zukunftsbezogen sind, kann das nichts daran ändern, dass sie personenbezogenen Daten sind. Gerade Prognose- und Planungsdaten berühren die Arbeitssituation der Person maßgeblich: Wird berechnet, dass die Weiterbildungschancen der Arbeitnehmerin in dem Unternehmen gering sind, wird die Arbeitnehmerin auch nicht mehr gefördert werden. Der sachliche Anwendungsbereich der DSGVO ist bei derartigen Informationen mithin eröffnet.

---

[86] Gola/Heckmann/*Gola*, Art. 4 DSGVO Rn. 14.

[87] *Eschholz*, DuD 2017, 180.

[88] Vgl. *Gärtner*, Smart HRM, 2020, S. 167.

[89] Vgl. *ders.*, Smart HRM, 2020, S. 167.

[90] Vgl. *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018, S. 123.

[91] S. dazu: Kapitel 5 A.III.1.a) (S. 63).

[92] *Art. 29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (WP 136), S. 11.

(2) Identifizierte oder identifizierbare Person

Die entsprechenden Daten sind aber nur als personenbezogene Daten einzustufen, wenn sie einer konkreten Person zugeordnet werden können.[93] Die Informationen müssen sich deshalb auf eine identifizierte oder identifizierbare Person beziehen.

Eine Person ist identifiziert, wenn die Identität einer Person unmittelbar aus der Information selbst folgt, d. h. etwa aus dem Namen, der Anschrift oder dem Geburtsdatum einer Person.[94]

Identifizierbar ist eine natürliche Person auch dann, wenn eine Information alleine noch für keine Zuordnung einer bestimmten Person ausreicht, sondern diese erst gelingt, wenn weitere Informationen dazukommen.[95] Das ist gem. Art. 4 Nr. 1 DSGVO der Fall, wenn die Person direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(3) Ganz und teilweise automatisierte Verarbeitung

Die personenbezogenen Daten müssen ganz oder teilweise automatisiert verarbeitet werden. Verarbeitung wird in Art. 4 Nr. 2 DSGVO definiert als „jede[r] mit oder ohne Hilfe automatisierter Verfahren ausgeführt[e] Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die

---

[93] Gola/Heckmann/*Gola*, Art. 4 DSGVO Rn. 14; *Mantz/Marosi*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 3 Rn. 12.

[94] Kühling/Buchner/*Klar/Kühling*, Art. 4 DSGVO Rn. 18.

[95] Kühling/Buchner/*dies.*, Art. 4 DSGVO Rn. 19.

Einschränkung, das Löschen oder die Vernichtung". Der Verarbeitungsbegriff ist mithin sehr weit gefasst.

Eine vollständig automatisierte Verarbeitung liegt vor, wenn die Datenverarbeitung unter Einsatz eines gesteuerten Verfahrens selbstständig abläuft. In Abgrenzung zu teilweise automatisierten Verarbeitungen sind keine händischen Zwischenschritte von einem Menschen erforderlich wie etwa das Eingeben der Daten in ein System.[96]

bb) Nichtautomatisierte Verarbeitung

Die DSGVO gilt auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Ein Dateisystem ist gem. Art. 4 Nr. 6 DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Soweit Akten oder Aktensammlungen sowie die Deckblätter nicht nach bestimmten Kriterien geordnet sind, fallen sie nicht in den Anwendungsbereich der DSGVO.[97]

Das Tatbestandsmerkmal „gespeichert werden sollen" ist weit zu verstehen.[98] Ein zielgerichtetes Verhalten ist nicht erforderlich; es reicht aus, wenn geplant ist, dass Dateien in ein Dateisystem aufgenommen werden, die Entscheidung aber noch vom Eintritt von Bedingungen, wie z. B. der Entscheidung der Personalleiterin, abhängt.[99]

In der Regel ist die DSGVO somit auch bei nicht automatisierter Verarbeitung anwendbar. Für den Untersuchungsgegenstand dieser Arbeit ist

---

[96] Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 6.
[97] Erwägungsgrund 15 S. 3 DSGVO.
[98] Paal/Pauly/*Ernst*, Art. 2 DSGVO Rn. 10.
[99] Paal/Pauly/*ders.*, Art. 2 DSGVO Rn. 10.

das aber nicht relevant: Bei Entscheidungen durch algorithmische Systeme werden die Daten ganz oder teilweise automatisiert verarbeitet.

b) Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich ist gem. Art. 1 Abs. 1 DSGVO auf natürliche Personen beschränkt. Personenbezogene Daten juristischer Personen sind grundsätzlich nicht nach der DSGVO geschützt.[100] Solche Daten sind nur geschützt, wenn sie einen Bezug zu einer natürlichen Person aufweisen.[101]

Nach Art. 2 Abs. 2 DSGVO werden bestimmte Tätigkeiten von der Verordnung ausgenommen: Werden personenbezogene Daten für persönliche oder familiäre Tätigkeiten oder für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten verarbeitet (Art. 2 Abs. 2 lit. c und d DSGVO), ist die DSGVO nicht anwendbar.

c) Räumlicher Anwendungsbereich

aa) Niederlassungsprinzip

Der Anwendungsbereich ist in räumlicher Hinsicht gem. Art. 3 Abs. 1 DSGVO eröffnet, wenn die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung einer Verantwortlichen oder einer Auftragsverarbeiterin in der Union erfolgt.[102] An die Voraussetzung der Niederlassung sind keine hohen Anforderungen zu stellen.[103] Es muss lediglich eine Tätigkeit durch eine feste Einrichtung effektiv und tatsächlich ausgeübt werden.[104]

Die Verarbeitung muss „im Rahmen der Tätigkeiten" der Niederlassung erfolgen. Entscheidend sind hierbei Maß und Umfang der Beteiligung der Niederlassung an den Aktivitäten, in deren Kontext personenbezogene Daten

---

[100] Ehmann/Selmayr/*Klabunde*, Art. 4 DSGVO Rn. 14; Taeger/Gabel/*Schmidt*, Art. 1 DSGVO Rn. 14.

[101] *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, C. II. 4. Rn. 317.

[102] Umfassend zum räumlichen Anwendungsbereich s. *Golland*, DuD 2018, 351.

[103] Vgl. Gola/Heckmann/*Piltz*, Art. 3 DSGVO Rn. 11 ff.

[104] Erwägungsgrund 22 DSGVO.

verarbeitet werden.[105] Die Niederlassung muss in die Datenverarbeitung mit einbezogen sein.[106] Die Anforderungen an das Merkmal sind jedoch ebenfalls nicht hoch: Das Datenschutzrecht soll einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte Einzelner gewähren.[107] Deshalb ließ es der EuGH in der Entscheidung *Google Spain*, die zur DSRL erging, ausreichen, dass die Niederlassung mit der eigentlichen Datenverarbeitung untrennbar verbunden war.[108]

Es kommt zudem nicht darauf an, ob die personenbezogenen Daten in der Union verarbeitet werden.[109] Mithin ist die DSGVO auch einschlägig, wenn ein in ihr niedergelassenes Unternehmen die personenbezogenen Daten z. B. in den USA verarbeitet.

bb) Marktortprinzip

Die DSGVO hat einen extraterritorialen Geltungsanspruch. [110] Als Verantwortlicher kann man sich nicht dem Anwendungsbereich der DSGVO entziehen, wenn man in einem Drittstaat niedergelassen ist und die Verarbeitung dort stattfindet. Gem. Art. 3 Abs. 2 DSGVO ist die Verordnung anwendbar, wenn die Verantwortliche oder die Auftragsverarbeiterin nicht in der Union niedergelassen ist. Außerdem müssen sich die betroffenen Personen, deren personenbezogene Daten verarbeitet werden, in der Union befinden und die Verarbeitung muss damit in Zusammenhang stehen, dass der betroffenen Person in der Union Waren oder Dienstleistungen angeboten werden (Art. 3 Abs. 2 lit. a DSGVO) oder das Verhalten der betroffenen Person in der Union beobachtet wird (Art. 3 Abs. 2 lit. b DSGVO).

Das Merkmal des „Angebots“ nach Art. 3 Abs. 2 lit. a DSGVO ist erfüllt, wenn die Verantwortliche oder Auftragsverarbeiterin „offensichtlich

---

[105] Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 55.

[106] Kühling/Buchner/*ders.*, Art. 3 DSGVO Rn. 55.

[107] EuGH, 13.5.2014 – C-131/12, *Google Spain SL und Google Inc. ./. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*, NJW 2014, 2257, 2260 Rn. 58.

[108] EuGH, 13.5.2014 – C-131/12, *Google Spain SL und Google Inc. ./. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*, NJW 2014, 2257, 2260 Rn. 56.

[109] Erwägungsgrund 22 DSGVO.

[110] *Uecker*, ZD 2019, 67.

beabsichtigt“ [111], betroffenen Personen in einem Mitgliedstaat oder in mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten. Ob ein „offensichtliches Beabsichtigen“ vorliegt, ist im Einzelfall zu prüfen.[112] Es ist nicht erforderlich, dass ein Vertrag abgeschlossen wird; auf der anderen Seite reicht es nicht aus, wenn eine Website, E-Mail-Adresse oder andere Kontaktdaten nur zugänglich sind.[113] Wird aber eine Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, verwendet, verbunden mit der Möglichkeit, Waren und Dienstleistung in dieser anderen Sprache zu bestellen, können das Anhaltspunkte sein, dass ein Angebot vorliegt.[114] Ein Angebot liegt jedenfalls nicht vor, wenn es nur unabsichtlich oder zufällig erfolgt.[115] Das Angebot kann auch mündlich oder schriftlich erfolgen.[116]

Eine betroffene Person wird i. S. d. Art. 3 Abs. 2 lit. b DSGVO beobachtet, wenn ihre Internetaktivitäten nachvollzogen werden, um z. B. von der Person anhand der Daten ein Profil zu erstellen, welches die Grundlage der sie betreffenden Entscheidungen bildet oder welches persönliche Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorhersagt. [117] Erwägungsgrund 24 S. 2 DSGVO sieht als Gegenstand der Beobachtung die „Internetaktivitäten“ der Personen vor. Unternehmensintern gewonnene Daten basieren typischerweise nicht oder jedenfalls nicht ausschließlich auf den Internetaktivitäten der Personen.[118] Im Wortlaut von Art. 3 Abs. 2 lit. b DSGVO ist eine Beschränkung auf Internetaktivitäten allerdings nicht verankert. Es ist davon auszugehen, dass Erwägungsgrund 24 DSGVO lediglich den wichtigsten Fall der Beobachtung beschreibt.[119] Wenn die im Internet gewonnenen Daten, die zur Profilerstellung genutzt werden, vom räumlichen Anwendungsbereich der Verordnung erfasst sind, müssen

---

[111] Erwägungsgrund 23 S. 2 DSGVO.
[112] Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 81.
[113] Gola/Heckmann/*Piltz*, Art. 3 DSGVO Rn. 38 f.
[114] Erwägungsgrund 23 S. 3 DSGVO.
[115] Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 81.
[116] Gola/Heckmann/*Piltz*, Art. 3 DSGVO Rn. 40.
[117] Erwägungsgrund 24 S. 2 DSGVO.
[118] Kühling/Buchner/*Klar*, Art. 3 DSGVO Rn. 93.
[119] NK-Datenschutzrecht/*Hornung*, Art. 3 DSGVO Rn. 58.

unternehmensintern gewonnene Daten, die entsprechend verarbeitet werden, erst recht unter den Anwendungsbereich der Verordnung fallen.[120]

cc) Völkerrecht

Unterliegt ein nicht in der Union niedergelassener Verantwortlicher einem Ort, der aufgrund des Völkerrechts dem Recht eines Mitgliedsstaats unterliegt, ist die Verordnung gem. Art. 3 Abs. 3 DSGVO ebenfalls anzuwenden. Damit sind Orte betroffen, die nach Völkerrecht nicht dem Drittstaat unterliegen, dem sie eigentlich zugehörig sind.[121] Das sind insbesondere diplomatische und konsularische Vertretungen von Mitgliedstaaten im Ausland.[122] Für den Untersuchungsgegenstand der Arbeit ist das jedoch nicht relevant.

3. Zwischenergebnis: weiter Anwendungsbereich der DSGVO

1. Die DSGVO hat sowohl einen weiten sachlichen als auch einen weiten räumlichen Anwendungsbereich. Die Verordnung differenziert nicht zwischen verschiedenen Anwendungsszenarien, für die personenbezogene Daten verarbeitet werden. Vielmehr kommt es allein darauf an, dass überhaupt personenbezogene Daten verarbeitet werden. Personenbezogene Daten liegen auch vor, wenn die Daten zukunftsbezogen sind. Für den Personenbezug reicht es aus, dass die Person identifizierbar ist. Werden Daten von Arbeitnehmerinnen oder Bewerberinnen verarbeitet, so liegen personenbezogene Daten vor, es sei denn, die Daten sind anonymisiert.[123]

2. Räumlich anwendbar ist die DSGVO, wenn personenbezogene Daten im Rahmen der Tätigkeiten einer Niederlassung einer Verantwortlichen oder Auftragsverarbeiterin in der Union verarbeitet werden.[124] Die

---

[120] *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018, S. 137 f.; NK-Datenschutzrecht/*Hornung*, Art. 3 DSGVO Rn. 58; Gola/Heckmann/*Piltz*, Art. 3 DSGVO Rn. 42.

[121] Paal/Pauly/*Ernst*, Art. 3 DSGVO Rn. 21.

[122] Taeger/Gabel/*Schmidt*, Art. 3 DSGVO Rn. 34; Erwägungsgrund 25 DSGVO.

[123] S. dazu sogleich unter: Kapitel 6 B.II. (S. 121).

[124] Kapitel 5 A.III.2.c) (S. 70).

Verarbeitung der Daten muss aber nicht in der Union stattfinden. Ist die Verantwortliche oder der Auftragsverarbeiterin nicht in der Union niedergelassen, ist der Anwendungsbereich dennoch eröffnet, wenn etwa die Datenverarbeitung im Zusammenhang damit steht, dass das Verhalten betroffener Personen in der Union beobachtet wird. Dabei sind nicht nur Daten, die aufgrund von Internetaktivitäten gesammelt werden, sondern auch unternehmensintern gewonnene Daten erfasst. Die DSGVO ist somit auch in fast allen Fällen räumlich anwendbar. Es muss lediglich ein Bezug zur Union vorliegen, sei es aufgrund der Niederlassung der Verantwortlichen oder der Auftragsverarbeiterinnen oder sei es, weil das Verhalten betroffener Personen in der Union erfolgt. Das wird auf die Herstellerinnen algorithmischer Systeme und auf die Verantwortlichen, die solche Systeme einsetzen, in aller Regel zutreffen. Der weite räumliche Anwendungsbereich der DSGVO führt dazu, dass man derartige Systeme nicht einfach ins Ausland auslagern kann, um dem Anwendungsbereich der DSGVO zu entfliehen.

3. Der Anwendungsbereich der DSGVO ist daher für algorithmische Systeme, die im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis eingesetzt werden und die personenbezogenen Daten der Bewerberinnen oder Arbeitnehmerinnen verarbeiten, in aller Regel sowohl in sachlicher, als auch persönlicher und räumlicher Hinsicht eröffnet.[125]

IV. KI-VO: Regulierung von KI auf unionaler Ebene

1. Hintergrund und Stand des Gesetzgebungsverfahrens

Der KI-VO-KOM wurde am 21. April 2021 von der Europäischen Kommission veröffentlicht. Er geht auf das politische Engagement von Frau von der Leyen, Präsidentin der Europäischen Kommission zurück, die bereits in den politischen Leitlinien für die Kommission verlauten ließ: „In my first 100 days in office, I will put forward legislation for a coordinated European

[125] Kühling/Buchner/*Herbst*, Art. 4 DSGVO Rn. 17.

approach on the human and ethical implications of Artificial Intelligence."[126] Bereits am 19. Februar 2020 veröffentlichte die Kommission ihr „Weißbuch zur KI – ein europäisches Konzept für Exzellenz und Vertrauen"[127], welches ein Konzept zur Regulierung von KI enthält. Die Kommission unterstützt danach „ein auf Regulierung und Finanzierung ausgerichtetes Konzept, das die Nutzung von KI fördert und gleichzeitig auf die mit dieser Technologie einhergehenden Gefahren eingeht"[128]. In dem Weißbuch werden politische Optionen vorgestellt, die diese Ziele verwirklichen sollen. Zum Weißbuch gab es eine öffentliche Konsultation, in der über 1.500 Beiträge aus aller Welt eingingen.[129] Nicht nur diese Beiträge, sondern auch diverse Studien wie z. B. der Bericht der Datenethikkommission [130] wurden im KI-VO-KOM berücksichtigt. Der KI-VO-KOM soll nun einen einheitlichen Rechtsrahmen für eine vertrauenswürdige KI schaffen.

Nachdem die Kommission am 21. April 2021 den KI-VO-KOM veröffentlicht hat, folgte zunächst ein Konsultationszeitraum, in dem 304 Nichtregierungsorganisationen befragt wurden. [131] Nach verschiedenen Kompromisstexten der französischen Ratspräsidentschaft sowie diversen Stellungnahmen wurde am 6. Dezember 2022 der KI-VO-RAT veröffentlicht. Der KI-VO-RAT unterscheidet sich an einigen Stellen wesentlich vom ursprünglichen Entwurf der Kommission. Am 14. Juni 2023 hat das Parlament den KI-VO-PARL veröffentlicht, der in größerem Umfang vom KI-VO-KOM abweicht.

Nun wird im Plenum unter Mitwirkung des Parlaments, der EU-Kommission und des Rates der Europäischen Union verhandelt (Trilog-Verhandlungen[132]).

---

[126] Political Guidelines for the next European Comission 2019-2024, S. 13, https://perma.cc/TA6T-NNLG (archiviert am 08.11.2022).

[127] *Europäische Kommission*, Weißbuch, 2020.

[128] *Dies.*, Weißbuch, 2020, S. 1.

[129] *Orssich*, EuZW 2022, 254, 255.

[130] *Datenethikkommission*, Gutachten der Datenethikkommission, 2019.

[131] Einen guten Überblick über den Gesetzgebungsprozess bietet der Gesetzgebungs-Tracker der Kanzlei Taylor Wessing: https://perma.cc/LD2D-VMHZ (archiviert am 08.11.2022).

[132] S. dazu: Calliess/Ruffert/*Kluth*, Art. 294 AEUV Rn. 26; *Bauerschmidt*, JuS 2022, 626, 629.

Sollte die KI-VO 2024 in Kraft treten, ist sie nach einer zweijährigen Übergangsfrist vermutlich 2026 anwendbar.

Der KI-VO-KOM bildet die Diskussionsgrundlage für die weiteren Organe der Europäischen Union sowie der Mitgliedstaaten. Deshalb dient der KI-VO-KOM als Grundlage der Untersuchung, wobei er stets in Bezug zum KI-VO-RAT sowie zum KI-VO-PARL gesetzt wird. Wenn sich keine wesentlichen Unterschiede zwischen den drei Vorschlägen ergeben, wird nur der KI-VO-KOM erwähnt. Die Bewertung der unterschiedlichen Regelungen folgt im vierten Teil der Arbeit.[133]

2. Verhältnis einer zukünftigen KI-VO zur DSGVO

Die DSGVO ist nur bei der Verarbeitung personenbezogener Daten anwendbar. Der KI-VO-KOM ist hingegen nicht auf die Verarbeitung personenbezogener Daten beschränkt, sondern erfasst unabhängig vom Personenbezug der verarbeiteten Daten verschiedene KI-Systeme (Art. 3 Nr. 1 KI-VO-KOM).

Die Regelungen der DSGVO sollen von einer zukünftigen KI-VO unberührt bleiben[134], werden aber teilweise durch den Entwurf ergänzt, insbesondere im Bereich der Trainingsdaten. [135] Zudem sind Verarbeitungen besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) gem. Art. 10 Abs. 5 KI-VO-KOM unter bestimmten Voraussetzungen gestattet.[136] Art. 54 Abs. 1 KI-VO-KOM sieht außerdem vor, dass personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme im Reallabor unter bestimmten Bedingungen (Art. 54 Abs. 1 lit. a-j KI-VO-KOM) weiterverarbeitet werden dürfen.[137]

---

[133] Kapitel 10 (S. 341); Kapitel 11 (S. 363).
[134] S. dazu Erwägungsgrund 2b KI-VO-PARL, S. 9.
[135] S. dazu: Kapitel 10 B.I. (S. 345).
[136] S. dazu: Kapitel 11 B. (S. 371).
[137] S. dazu: Kapitel 11 E. (S. 384).

3. Anwendungsbereich einer zukünftigen KI-VO

a) Sachlicher Anwendungsbereich einer zukünftigen KI-VO

Sachlich anwendbar ist der KI-VO-KOM auf KI-Systeme. Ein KI-System ist nach Art. 3 Nr. 1 KI-VO-KOM eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf verschiedene vom Menschen festgelegte Ziele, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld, mit dem sie interagieren, beeinflussen. Nach Anhang I sind KI-Systeme im Sinne des KI-VO-KOM nicht nur solche, die auf der Grundlage von maschinellem Lernen entwickelt worden sind, sondern auch solche, die auf statistischen Methoden beruhen. Mithin werden vom KI-VO-KOM auch derartige Software-Systeme erfasst, die nicht mithilfe von KI entwickelt worden sind.[138]

Der KI-VO-Rat sieht hingegen vor, die Definition von KI-Systemen auf Systeme einzugrenzen, die anhand von Konzepten des maschinellen Lernens sowie logik- und wissensgestützten Konzepten entwickelt wurden. [139] Außerdem ist ein KI-System so konzipiert, dass es mit Elementen der Autonomie arbeitet (Art. 3 Nr. 1 KI-VO-RAT). Es wird allerdings nicht weiter definiert, was unter „Elementen der Autonomie" zu verstehen ist.

Im KI-VO-PARL wird eine ähnliche Position vorgeschlagen (Art. 3 Nr. 1 KI-VO-PARL). Demnach ist ein KI-System ein maschinengestütztes System, das so konzipiert ist, dass es mit einem unterschiedlichen Grad an Autonomie arbeitet und für explizite oder implizite Ziele Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen erzeugen kann, die die physische oder virtuelle Umgebung beeinflussen. Außerdem differenziert der KI-VO-PARL zwischen einem sog. *foundation model* (Basismodell), einem sog. *general purpose AI system* (KI-System für allgemeine Zwecke) und einer sog. *generative AI* (generative KI). Gem. Art. 3 Abs. 1 Nr. 1 lit. c KI-VO-PARL ist ein Basismodell ein KI-System, das auf der Grundlage umfangreicher Daten trainiert wurde, auf die Allgemeinheit der Ergebnisse auslegt ist und an ein

---

[138] Zum KI-Begriff in dieser Arbeit s. Kapitel 1 (S. 9).

[139] KI-VO-RAT, S. 4.

breites Spektrum unterschiedlicher Aufgaben angepasst werden kann. Ein KI-System für allgemeine Zwecke ist gem. Art. 3 Abs. 1 Nr. 1 lit. d KI-VO-PARL ein KI-System, das in einem breiten Spektrum von Anwendungen eingesetzt und an diese angepasst werden kann, für die es jedoch nicht absichtlich und speziell entwickelt wurde. Schließlich ist ein generatives KI-System ein KI-System, welches ausdrücklich dafür vorgesehen ist, mit unterschiedlichen Leveln an Anonymität, Inhalte wie komplexe Texte, Bilder, Audios oder Videos zu generieren (Art. 28b Abs. 4 KI-VO-PARL). Für Anbieterinnen von Basismodellen sieht der KI-VO-PARL besondere Anforderungen vor. Eine trennscharfe Abgrenzung zwischen den drei genannten Systemen ist kaum möglich. Ein Basismodell wird in der Regel auch ein generatives KI-System sein. Häufig wird es gleichzeitig auch ein KI-System für allgemeine Zwecke sein. Jedenfalls erfüllt der Begriff des KI-Systems für allgemeine Zwecke keinen eigenen Mehrwert, weil ein KI-System für allgemeine Zwecke zumeist auch ein generatives KI-System ist. Der Begriff des KI-Systems für allgemeine Zwecke sollte daher aufgegeben werden.[140]

Die Definitionen des KI-VO-PARL erfassen aber jedenfalls auch Systeme wie ChatGPT, die die Diskussion rund um generative KI neu aufgeworfen haben. Der KI-VO-KOM hatte solche KI-Systeme bislang nicht hinreichend abgedeckt. Zum anderen sind die neuen Definitionsvorschläge eine Reaktion auf die vielfach geäußerte Kritik, dass der Begriff der KI nicht spezifisch genug definiert sei.[141] Mit einer wie im KI-VO-KOM vorgeschlagenen Definition würden fast alle Systeme erfasst werden, auch wenn sie etwa bloß mit

---

[140] *Hacker*, Stellungnahme für die Öffentliche Anhörung „Generative Künstliche Intelligenz" am Mittwoch, 24. Mai 2023, 14:30 – 16:30 Uhr, Sitzungssaal Reichstagsgebäude (RTG) 3 N 001, S. 2.

[141] *Abbou*, Schriftliche Stellungnahme für die am 26.09.2022 stattfindende Anhörung des Ausschusses für Digitales zur EU-Verordnung zu Künstlicher Intelligenz unter Einbeziehung Wettbewerbsfähigkeit im Bereich Künstliche Intelligenz und Blockchain-Technologie, S. 1; *Algorithm Watch*, Draft AI Act: EU needs to live up to its own ambitions in terms of governance and enforcement, 2021, S. 2 ff.; *Gless/Janal*, in: Hilgendorf/Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur künstlichen Intelligenz, 2023, S. 24 Rn. 32; *Ebers/Hoch/Rosenkranz u.a.*, RDi 2021, 528, 529.

statistischen Methoden arbeiten würden und daher nicht im eigentlichen Sinne[142] mit künstlicher Intelligenz funktionieren.

b) Persönlicher und räumlicher Anwendungsbereich einer zukünftigen KI-VO

Der persönliche und räumliche Anwendungsbereich einer zukünftigen KI-VO erstreckt sich gem. Art. 2 Abs. 1 KI-VO-KOM auf

- Anbieterinnen, die KI-Systeme in der Union in den Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieterinnen in der Union oder in einem Drittland niedergelassen sind (Art. 2 Abs. 1 lit. a KI-VO-KOM);
- Nutzerinnen von KI-Systemen, die sich in der Union befinden (Art. 2 Abs. 1 lit. b KI-VO-KOM);
- Anbieterinnen und Nutzerinnen von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird (Art. 2 Abs. 1 lit. c KI-VO-KOM).

Erfasst sind somit alle KI-Systeme, die in der Union genutzt oder angeboten werden sollen. Ausreichend ist aber bereits, wenn das Ergebnis des Systems in der Union verwendet wird. Anbieterinnen sollen sich nicht dem Regelungsregime der Union entziehen, indem sie ihren Firmensitz in einen Drittstaat verlagern.[143]

Im KI-VO-RAT ist der Anwendungsbereich sogar noch größer: Nach Art. 2 Abs. 1 lit. c KI-VO-RAT müssen die Anbieterin und Nutzerin nicht in einem Drittland niedergelassen oder ansässig sein, sondern es reicht aus, wenn sie in einem Drittland physisch anwesend sind. Während eine Niederlassung oder eine Ansässigkeit mit einer zeitlichen Dauer einhergeht, kann physische Anwesenheit auch eine kürzere zeitliche Spanne umfassen. Außerdem soll die Verordnung nach dem KI-VO-RAT auch für Einführerinnen und Händlerinnen von KI-Systemen (Art. 2 Abs. 1 lit. d KI-VO-RAT), für Produktherstellerinnen, die KI-Systeme zusammen mit ihrem Produkt unter

---

[142] Zum KI-Begriff in dieser Arbeit s. Kapitel 1 (S. 9).
[143] Vgl. *Schlee*, ZD-Aktuell 2021, 05194.

ihrem Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen (Art. 2 Abs. 1 lit. e KI-VO-RAT), sowie für Bevollmächtigte von Anbieterinnen, die in der Union niedergelassen sind (Art. 2 Abs. 1 lit. f KI-VO-RAT), gelten.

Der KI-VO-PARL ändert den Begriff der Nutzerinnen von KI-Systemen zu *Bereitstellerinnen*, die sich in der Union befinden oder dort ihren Sitz haben (Art. 2 Abs. 1 lit. b KI-VO-PARL).[144] Außerdem soll die KI-VO nach Art. 2 Abs. 1 lit. c KI-VO-PARL bereits dann anwendbar sein, wenn das vom System generierte Ergebnis dafür vorgesehen ist, in der Union verwendet zu werden. Mithin reicht auch die bloße Absicht aus, das Ergebnis zu verwenden, es muss nicht tatsächlich – wie vom KI-VO-KOM vorgeschlagen – verwendet werden. Diese Differenzierung ist insofern sinnvoll, weil die Vorgaben der zukünftigen KI-VO dann auch bereits vor der tatsächlichen Verwendung des Ergebnisses eines KI-Systems greifen und nicht erst dann, wenn das Ergebnis tatsächlich verwendet wird. Das überzeugt: Die Regelungen für bestimmte KI-Systeme sollten auch sinnvollerweise bereits vor dem tatsächlichen Einsatz des Systems anwendbar sein und nicht erst dann, wenn das System schon eingesetzt wird.

4. Ziele einer zukünftigen KI-VO

Die konkreten Ziele des KI-VO-KOM sind folgende:[145]

- KI-Systeme, die im europäischen Markt existieren und genutzt werden, sollen sicher sein und die bestehenden Grundrechte sowie Werte der Union wahren.
- Um Investitionen in KI und innovative KI zu fördern, soll Rechtssicherheit gewährleistet sein.
- Governance und die wirksame Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie die Sicherheitsanforderungen an KI-Systeme sollen gestärkt werden.

---

[144] Zum Begriff der Nutzerinnen und Bereitstellerinnen s. Kapitel 10 A. (S. 341).
[145] KI-VO-KOM, S. 3.

- Die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Systeme muss erleichtert werden; eine Marktfragmentierung soll verhindert werden.

Damit die Ziele umgesetzt werden können, wird gem. den Art. 56 ff. KI-VO-KOM ein „European Artificial Intelligence Board" eingerichtet. Dieser Ausschuss soll die Kommission zu verschiedenen Zwecken beraten und unterstützen. Dazu gehört etwa, an Leitlinien mitzuwirken sowie die nationalen Aufsichtsbehörden und die Kommission bei der einheitlichen Anwendung der Verordnung zu unterstützen (Art. 56 Abs. 2 KI-VO-KOM). Der Ausschuss setzt sich gem. Art. 57 Abs. 1 KI-VO-KOM aus den nationalen Aufsichtsbehörden, vertreten durch ihre Leiterinnen, einer gleichwertig hochrangigen Beamtin der Behörde und der Europäischen Datenschutzbeauftragten zusammen. Im KI-VO-RAT werden die Anforderungen an den Ausschuss weiter präzisiert. Etwa müssen die Mitgliedstaaten dafür sorgen, dass die Vertreterinnen im KI-Ausschuss über die einschlägigen Kompetenzen und Befugnisse verfügen, um die Aufgaben des Ausschusses bewältigen zu können.[146] Außerdem sieht der KI-VO-RAT eine andere Besetzung des Ausschusses vor: Der Ausschuss soll sich aus einer Vertreterin je Mitgliedstaat zusammensetzen (Art. 56 Abs. 2 KI-VO-RAT). Die Europäische Datenschutzbeauftrage soll als Beobachterin teilnehmen. Auch die Kommission soll an den Sitzungen teilnehmen, sich aber nicht an den Abstimmungen beteiligen. Je nach Relevanz der Fragestellungen können auch Behörden, Gremien oder Sachverständige der Mitgliedstaaten und der Union im Einzelfall zu den Sitzungen des Ausschusses eingeladen werden. Art. 57 Abs. 1 KI-VO-PARL ergänzt Art. 57 Abs. 1 KI-VO-KOM dahingehend, dass auch KI-Ethik-Expertinnen und Vertreterinnen der Industrie im Ausschuss sitzen. Andere nationale, regionale und lokale Behörden können zu den Sitzungen eingeladen werden, wenn die erörterten Themen für sie von Bedeutung sind. Die Ergänzungen des KI-VO-RAT und des KI-VO-PARL sind sinnvoll. Insbesondere, dass KI-Ethik-Expertinnen und ggf. auch Sachverständige herangezogen werden können, ist unabdingbar, um bei den Entscheidungen und Diskussionen zu Ergebnissen zu kommen.

[146] KI-VO-RAT, S. 151.

Vorgesehen ist zudem ein „*robust monitoring and evaluation mechanism*“, um sicherzustellen, dass die im KI-VO-KOM genannten Ziele erreicht werden. Aus diesem Grund soll eine EU-weite Datenbank angelegt werden, um KI-Systeme mit hohem Risiko zu registrieren (Art. 60 KI-VO-KOM). Der EU-Datenbank sollen Nutzerinnen und Interessierte auch entnehmen können, ob das KI-System mit der Verordnung übereinstimmt. Art. 60 Abs. 3 KI-VO-PARL ergänzt, dass die in der EU-Datenbank enthaltenen Informationen für die Öffentlichkeit zugänglich, benutzerfreundlich, leicht navigier- und maschinenlesbar sein müssen.

5. Risikobasierter Ansatz einer zukünftigen KI-VO

Der KI-VO-KOM ist ein präventives Verbotsgesetz mit Erlaubnisvorbehalt.[147] Je nach Risikostufe ist ein KI-System unterschiedlichen regulatorischen Anforderungen unterworfen – oder im Falle der höchsten Risikostufe – vollständig verboten. Der KI-VO-KOM unterscheidet zwischen drei Kategorien: KI-Systemen mit a) unannehmbaren Risiken, b) hohen Risiken und c) geringen oder minimalen Risiken.[148] Der KI-VO-RAT nimmt zusätzlich noch KI-Systeme mit allgemeinem Verwendungszweck auf, für die abgestufte Pflichten gelten sollen.[149] Art. 28b KI-VO-PARL regelt besondere Pflichten für Anbieterinnen von sog. *foundation models*. Die grundsätzliche Klassifizierung nach Risikostufen ändert sich mithin im KI-VO-RAT und KI-VO-PARL nicht.

6. Zwischenergebnis: Algorithmische Systeme von einer zukünftigen KI-VO erfasst

1. Algorithmische Systeme, die im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis eingesetzt werden, sind vom KI-VO-KOM erfasst. Auch wenn der KI-VO-RAT und der KI-VO-PARL ergänzende und abweichende Regelungen vorsehen, werden algorithmische Systeme auch von einer finalen KI-VO erfasst. Gem. Annex III Nr. 4 KI-VO-KOM sind KI-Systeme, die für Bewerbungsprozesse oder die Auswahl natürlicher Personen,

---

[147] Vgl. *Bomhard/Merkle*, RDi 2021, 276, 277.
[148] KI-VO-KOM, S. 12.
[149] KI-VO-RAT, S. 79 f.

insbesondere für die Bewertung von Kandidatinnen verwendet werden (Annex III Nr. 4 lit. a), oder solche, die für die Beendigung von Arbeitsverhältnissen oder Leistungsbewertung genutzt werden, Hochrisikosysteme (Annex III Nr. 4 lit. b). Diesen Systemen ist ein hohes Risiko für Sicherheit und Grundrechte inhärent.[150] Der KI-VO-RAT präzisiert den Anwendungsfall für derartige KI-Systeme und fasst unter Hochrisiko-KI-Systeme solche, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerberinnen zu bewerten (Anhang III Nr. 4 lit. a KI-VO-RAT). Außerdem sind KI-Systeme erfasst, die bestimmungsgemäß verwendet werden sollen, um über Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen zu entscheiden, die aufgrund des Verhaltens oder persönlicher Merkmale oder Eigenschaften Aufgaben zuweisen sowie die Leistung und das Verhalten von Personen in entsprechenden Beschäftigungsverhältnissen beobachten und bewerten (Anhang III Nr. 4 lit. b KI-VO-RAT). In Anhang III Nr. 4 lit. b KI-VO-PARL sind außerdem KI-Systeme aufgeführt, die Entscheidungen hinsichtlich Anbahnung, Beförderung und Beendigung von arbeitsbezogenen Vertragsverhältnissen wesentlich beeinflussen. Die Entscheidung muss mithin nicht von einem System getroffen werden, es reicht aus, wenn die (menschliche) Entscheidung beeinflusst ist. Diese Wertung ist richtig und wichtig: Die menschliche Entscheidung wird erheblich vom Ergebnis eines algorithmischen Systems beeinflusst.[151]

2. Die oben vorgestellten Anwendungsfälle[152] werden für die Auswahl oder Bewertung natürlicher Personen im Beschäftigungskontext eingesetzt. Es handelt sich teilweise um ein Filtern der Bewerberinnen verbunden mit einer Bewertung oder aber um die Auswertung der Leistung oder des Verhaltens der Bewerberinnen oder Arbeitnehmerinnen. All diese Anwendungsfälle fallen unter die oben genannten Definitionen des KI-VO-KOM und auch unter diejenigen

---

[150] *Orssich*, EuZW 2022, 254, 258.

[151] S. dazu: Kapitel 6 D.IV.3.b) (S. 216).

[152] Kapitel 2 (S. 23).

des KI-VO-RAT sowie des KI-VO-PARL. Die Vorschriften des KI-VO-KOM sind daher für Anwenderinnen der beschriebenen algorithmischen Systeme relevant. Geklärt werden muss aus rechtlicher Perspektive daher, wie die Vorschriften für die Vorgaben solcher Systeme verstanden werden und wie sich diese Vorschriften zur DSGVO verhalten.[153]

V. KI-HaftRL-E

1. Gesetzgeberischer Hintergrund

Am 28. September 2022 hat die Kommission einen Vorschlag für eine KI-Haftungsrichtlinie vorgelegt.[154] Zuvor hatte das Parlament am 20.10.2020 einen Verordnungsentwurf für eine Haftung von KI-Systemen präsentiert.[155] Mangels des fehlenden Initiativrechts des Europäischen Parlaments (s. Art. 17 EUV) kann es keine direkten Vorschläge in das Gesetzgebungsverfahren einbringen. Das Europäische Parlament kann aber gem. Art. 225 AEUV die Kommission auffordern, einen Gesetzesvorschlag zu erarbeiten. Daher ging man vor dem KI-HaftRL-E davon aus, dass ein Verordnungsentwurf für die Haftung von KI-Systemen von der Kommission vorgelegt werden würde.[156]

2. Inhalt des KI-HaftRL-E

Der KI-HaftRL-E gilt gem. Art. 1 Abs. 2 KI-HaftRL-E nur für außervertragliche verschuldensunabhängige zivilrechtliche Schadensersatzansprüche in Bezug auf Schäden, die durch ein KI-System verursacht worden sind. Die Begriffe KI-System, Hochrisiko-KI-System, Anbieterin und Nutzerin richten sich gem. Art. 2 Nr. 1-4 KI-HaftRL-E nach den im KI-VO-KOM genannten Definitionen.

---

[153] Dazu näher unter: Kapitel 11 (S. 363).

[154] Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM(2022)496 final.

[155] Europäisches Parlament, Entschließung vom 20.10.2020, P9_TA (2020)0276.

[156] *Burchardi*, EuZW 2022, 685.

Der KI-HaftRL-E nennt keine neuen Haftungstatbestände für KI, sondern enthält vielmehr Vorschriften über die Offenlegung von Beweismitteln bei Hochrisiko-KI-Systemen und über die Beweislast, wenn außervertragliche verschuldensabhängige zivilrechtliche Ansprüche vor nationalen Gerichten in Bezug auf Schäden, die durch ein KI-System verursacht wurden (Art. 1 Abs. 1 KI-HaftRL-E), gegeben sind.

3. Bedeutung des KI-HaftRL-E für den Untersuchungsgegenstand

Der Schwerpunkt dieser Arbeit liegt nicht darin, die Haftung für KI umfassend zu beleuchten. Einzig bei § 15 AGG könnte der Richtlinienentwurf relevant werden. Diese Norm regelt Schadensersatz und Entschädigungsansprüche des Beschäftigten bei einem Verstoß gegen das Benachteiligungsverbot nach § 7 AGG. Allerdings ist der Anspruch nach § 15 AGG als vertraglicher Anspruch zu qualifizieren.[157] Der Entwurf erfasst jedoch explizit nur außervertragliche Ansprüche. Somit ist der KI-HaftRL-E für den Untersuchungsgegenstand nicht weiter relevant.[158]

B. Nationale Ebene

Im nationalen Recht gibt es kein ausdrücklich normiertes Datenschutzgrundrecht. Vielmehr ergibt sich ein Schutz personenbezogener Daten aus dem Recht auf informationelle Selbstbestimmung, welches eine Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG ist.[159]

---

[157] MHdb ArbR Band 1/*Oetker*, § 14 Arbeitskollisionsrecht Rn. 82; Staudinger (2020) Einleitung AGG/*Serr*, Rn. 12.

[158] Zum Richtlinienentwurf s. etwa *Bomhard/Siglmüller*, RDi 2022, 506; *Eichelberger*, DB 2022, 2783.

[159] BVerfG, 19.4.2016 – 1 BvR 3309/13, NJW 2016, 1939-1945, 1942; ErfK/*Schmidt*, Art. 2 GG Rn. 41.

I. Recht auf informationelle Selbstbestimmung

1. Sachlicher Schutzbereich

Das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG, dessen Konturen erstmals im Volkszählungsurteil des BVerfG 1983[160] geformt worden sind, schützt die persönlichen Daten einer Person. Konkret wird die Einzelne gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten geschützt. [161] Grundsätzlich darf die Einzelne selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig.[162]

2. Persönlicher Schutzbereich

Jede natürliche Person kann sich auf das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts berufen.[163] Private sind grundsätzlich nicht an das Recht auf informationelle Selbstbestimmung gebunden. Im Wege der staatlichen Schutzpflicht können privaten Akteuren aber Schranken gesetzt werden, sofern eine Schutzpflichtlage besteht.[164]

Umstritten ist, ob sich auch juristische Personen sowie Gesamthandsgemeinschaften auf das allgemeine Persönlichkeitsrecht berufen

---

[160] BVerfG, 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, NJW 1984, 419.

[161] BVerfG, 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, NJW 1984, 419, 422; von Münch/Kunig/*Kunig/Kämmerer*, Art. 2 GG Rn. 75 f.

[162] BVerfG, 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, NJW 1984, 419, Ls.

[163] Dreier-Grundgesetz-Kommentar/*Barczak*, Art. 2 Abs. 1 GG Rn. 98.

[164] Dürig/Herzog/Scholz/*Di Fabio*, Art. 2 Abs. 1 GG Rn. 189.

können.[165] Das BVerfG differenziert je nach Ausprägung des Grundrechts.[166] Nach Art. 19 Abs. 3 GG gelten die Grundrechte für juristische Personen, soweit sie ihrem Wesen nach auf diese anwendbar sind. Daher kann auch für juristische Personen der Schutz des Rechts auf informationelle Selbstbestimmung gelten. Gleichwohl können sich juristischen Personen aber nur auf Art. 2 Abs. 1 GG berufen; die Menschenwürde nach Art. 1 Abs. 1 GG können nur natürliche Personen beanspruchen. [167] Juristische Personen können keine personale Würde haben.[168]

II. Einfachgesetzliche Grundlagen

1. Verhältnis des § 26 BDSG zu den Vorschriften der DSGVO

Auf einfachgesetzlicher Ebene hat der nationale Gesetzgeber § 26 BDSG für die Verarbeitung personenbezogener Daten im Beschäftigungskontext erlassen. Diese Norm beruht auf Art. 88 Abs. 1 DSGVO.[169] Art. 88 Abs. 1 DSGVO[170] enthält eine Öffnungsklausel für den Beschäftigtendatenschutz: Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext [...] vorsehen.

Gem. § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigen für Zwecke des Beschäftigungsverhältnisses u. a. verarbeitet werden, wenn dies für die Entscheidung über die Begründung, Durchführung, Beendigung eines Beschäftigungsverhältnisses erforderlich ist. § 26 Abs. 1 S. 2 BDSG regelt, unter welchen Voraussetzungen Daten von

---

[165] Dreier-Grundgesetz-Kommentar/*Barczak*, Art. 2 Abs. 1 GG Rn. 99.

[166] BVerfG, 13.6.2007 – 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05, NJW 2007, 2464, 2471 Rn. 152.

[167] BVerfG, 26.2.1997 – 1 BvR 2172/96, NJW 1997, 1841, 1843; Jarass/Pieroth/*Jarass*, Art. 1 GG Rn. 7.

[168] Jarass/Pieroth/*Jarass*, Art. 1 GG Rn. 7.

[169] ErfK/*Franzen*, § 26 BDSG Rn. 4; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 1; Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 9 ff.

[170] S. dazu näher unter: Kapitel 6 C.V. (S. 192).

Beschäftigten verarbeitet werden dürfen, wenn Straftaten aufgedeckt werden sollen. § 26 Abs. 2 BDSG enthält Anforderungen dafür, wenn die Daten aufgrund einer Einwilligung verarbeitet werden. In § 26 Abs. 3 BDSG ist geregelt, unter welchen Voraussetzungen sensible personenbezogene Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden dürfen. § 26 Abs. 4 BDSG bejaht die Möglichkeit, Kollektivvereinbarungen als Grundlage für die Verarbeitungen personenbezogener Daten zu nutzen. In § 26 Abs. 5 BDSG ist geregelt, dass die Verantwortliche geeignete Maßnahmen ergreifen muss, um die in Art. 5 DSGVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten einzuhalten. Während § 26 Abs. 6 DSGVO bislang vor allem klarstellende Bedeutung hatte, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben, weitet § 26 Abs. 7 den Anwendungsbereich der § 26 Abs. 1 bis BDSG auf die manuelle Datenverarbeitung aus. § 26 Abs. 8 BDSG enthält schließlich eine Legaldefinition des Beschäftigtenbegriffs.

§ 26 Abs. 1 S. 1 BDSG wurde bislang gegenüber dem Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. b DSGVO als *lex specialis* eingeordnet.[171]

Am 30. März 2023 befasste sich der EuGH im Rahmen eines Vorabentscheidungsverfahrens mit § 23 Abs. 1 S. 1 HDSIG.[172] Diese Norm ist wortgleich mit § 26 Abs. 1 S. 1 BDSG. Im Ergebnis hat der EuGH entschieden, dass § 23 Abs. 1 HDSIG und somit auch § 26 Abs. 1 S. 1 BDSG unanwendbar sind. Grund dafür ist, dass es sich aus Sicht des EuGH nicht um Vorschriften handelt, die „spezifischer" i. S. d. Art. 88 Abs. 1 DSGVO sind. Die Anforderungen, die eine nationale Vorschrift nach Art. 88 Abs. 1 DSGVO einhalten muss, sind nicht gewahrt. Im Folgenden wird das Urteil des EuGH vom 30. März 2023 eingeordnet und bewertet. Zudem werden die praktischen Folgen des Urteils erläutert.

---

[171] ErfK/*Franzen*, § 26 BDSG Rn. 5; Gola/Heckmann/*Pötters*, § 26 BDSG Rn. 4.

[172] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

a) § 26 Abs. 1 S. 1 BDSG als „spezifischere Vorschrift" i. S. d. Art. 88 Abs. 1 DSGVO?

Bereits vor dem Urteil des EuGH vom 30. März 2023 wurde in der Literatur zum Teil kritisiert, dass der nationale Gesetzgeber die Möglichkeit zu „spezifischeren Vorschriften" gem. Art. 88 Abs. 1 DSGVO nicht ausgenutzt habe.[173] Vielmehr sei die Norm gar keine „spezifischere Vorschrift", weil sie inhaltlich lediglich Art. 6 Abs. 1 S. 1 lit. b DSGVO wiederhole.[174] Dieser regelt, dass eine Verarbeitung personenbezogener Daten rechtmäßig ist, wenn die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist.

Ähnlicher Ansicht war auch das VG Wiesbaden[175]: Bei § 23 Abs. 1 S. 1 HDSIG (wortgleich mit § 26 Abs. 1 S. 1 BDSG) handele es sich nicht um eine Norm, die *lex specialis* zu Art. 6 Abs. 1 S. 1 lit. b DSGVO sei. Art. 88 Abs. 2 DSGVO sei nicht beachtet worden. Allein der in § 23 Abs. 5 HDSIG (entspricht § 26 Abs. 5 BDSG) enthaltene Hinweis, dass die Verantwortliche die Grundsätze des Art. 5 DSGVO einhalten müsse, genüge nicht den Vorgaben des Art. 88 Abs. 2 DSGVO. Das VG Wiesbaden hat daher dem EuGH in einem Vorabentscheidungsverfahren (Art. 267 AEUV) hinsichtlich der Auslegung von Art. 88 DSGVO zwei Fragen gestellt:[176] (1) Ist Art. 88 DSGVO dahin auszulegen, dass eine Rechtsvorschrift, um als spezifischere Vorschrift im Sinne von Art. 88 Abs. 1 DSGVO eingestuft werden zu können, die Vorgaben von Art. 88 Abs. 2 DSGVO erfüllen muss? (2) Welche Folgen hat die Feststellung, dass nationale Rechtsvorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext nicht mit den in Art. 88 Abs. 1 und 2 DSGVO vorgesehenen Voraussetzungen und Grenzen vereinbar sind?

---

[173] Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 2; *Franzen*, EuZA 2022, 261, 262.

[174] Vgl. dazu auch: *Schild*, ZD-Aktuell 2021, 5470.

[175] VG Wiesbaden, 21.12.2020 – 23 K 1360/20.WI.PV, ZD 2021, 394, 395.

[176] Zu den Vorlagefragen s. EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

b) § 26 Abs. 1 S. 1 BDSG erfüllt nicht die Anforderungen von Art. 88 Abs. 1 und 2 DSGVO

Am 30. März 2023 [177] hat der EuGH im oben genannten Vorabentscheidungsverfahren entschieden. Er hat entschieden, dass die Anforderungen an Art. 88 Abs. 2 DSGVO gewahrt sein müssen, um als spezifischere Vorschrift i. S. d. Art. 88 Abs. 1 DSGVO eingeordnet zu werden.[178] Das bedeutet, dass die Vorschriften in Bezug auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen müssen.[179]

Die von den Mitgliedstaaten erlassenen „spezifischeren Vorschriften" dürfen deshalb auch nicht den Wortlaut der in Art. 6 DSGVO genannten Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und der in Art. 5 DSGVO genannten Datenschutzgrundsätze wiederholen.[180]

Der EuGH kommt zu dem Schluss, dass nationale Vorschriften unangewendet bleiben müssen, wenn sie nicht die in Art. 88 Abs. 1 und 2 DSGVO geregelten Voraussetzungen und Grenzen beachten.[181]

Legt man diese Aussagen des EuGH zugrunde, sind § 23 Abs. 1 S. 1 HDSIG und mithin auch § 26 Abs. 1 S. 1 BDSG nicht mehr anzuwenden. Die Normen gehen von ihrem Regelungsgehalt nicht über Art. 6 Abs. 1 lit. b und c

---

[177] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[178] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 662 Rn. 65.

[179] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 663 Rn. 74.

[180] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 663 Rn. 71.

[181] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 664 Rn. 89.

DSGVO hinaus, sondern „wiederholen" vielmehr größtenteils den Wortlaut des Art. 6 Abs. 1 lit. b und c DSGVO.[182]

Sowohl § 23 Abs. 1 S. 1 HDSIG und auch § 26 Abs. 1 S. 1 BDSG enthalten keine besonderen Vorgaben dazu, um die Anforderungen des Art. 88 Abs. 2 DSGVO zu wahren. Es sind keine geeigneten und besonderen Maßnahmen vorgesehen, um die menschliche Würde, die berechtigten Interessen und die Grundrechte der betroffenen Person zu wahren. Sie sind deshalb nicht „spezifischer" i. S. d. Art. 88 Abs. 1 DSGVO.[183]

Die Auffassung des EuGH ist zu begrüßen.[184] Der EuGH argumentiert zum einen mit der Bedeutung des Wortlauts des Art. 88 Abs. 1 DSGVO. Eine Vorschrift sei nicht „spezifischer", wenn sie den Wortlaut einer anderen Vorschrift wiederhole. Das überzeugt vom Wortsinn her. Außerdem seien die Voraussetzungen des Art. 88 Abs. 2 DSGVO zu berücksichtigen. Diese Voraussetzungen müssten eingehalten werden, weil sie dem Ermessen der Mitgliedstaaten, die nach Art. 88 Abs. 1 DSGVO spezifischere Vorschriften erlassen können, einen Rahmen setzten. Das ist ebenfalls überzeugend: Würde man die Vorgaben des Art. 88 Abs. 2 DSGVO nicht bei Art. 88 Abs. 1 DSGVO berücksichtigen, würden diese Vorgaben keinen eigenen Zweck erfüllen.[185]

Die Entscheidung des EuGH ist aber auch insbesondere wegen des Regelungszwecks des Art. 88 DSGVO zutreffend. Mit der Öffnungsklausel wird den Mitgliedstaaten die Möglichkeit gegeben, im Beschäftigungskontext spezifischere Vorschriften zu treffen. Das bedeutet, dass sie konkrete Maßstäbe aufstellen können, wann eine Datenverarbeitung im Beschäftigungskontext rechtmäßig ist. Diese Entscheidung soll nach der Wertung der Öffnungsklausel dem Gesetzgeber und nicht den Gerichten überlassen sein. Momentan führt die offene Regelung des § 26 Abs. 1 S. 1 BDSG aber dazu, dass die Gerichte die spezifischeren nationalen Maßstäbe

---

[182] *Meinecke*, NZA 2023, 487, 493.

[183] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 663 Rn. 75.

[184] So auch: *Glocker/Hoffmann*, BB 2023, 1333, 1334.

[185] Vgl. Kapitel 6 C.V.2.b) (S. 199).

aufstellen. Die nationalen Gerichte müssen die nationalen Vorschriften – anders als die DSGVO selbst – nicht nach autonomen europäischen Maßstäben auslegen. Art. 88 DSGVO soll aber gerade nicht bewirken, dass aufgrund einer vom Wortlaut her ähnlich lautenden nationalen Regelung die autonome Auslegung faktisch umgangen wird.

c) § 26 Abs. 1 S. 1 BDSG ist unanwendbar

In der Konsequenz kann man Datenverarbeitungen im Beschäftigungskontext nicht mehr auf § 26 Abs. 1 S. 1 BDSG stützen. Vielmehr muss man die Rechtsgrundlagen des Art. 6 DSGVO heranziehen, solange es keine spezifischere Rechtsgrundlage für die Datenverarbeitung gibt.[186] Aus einem Positionspapier des BMAS und des BMI geht hervor, dass sie einen Entwurf für ein eigenständiges Beschäftigtendatenschutzgesetz vorlegen wollen.[187] Es ist davon auszugehen, dass ein solcher Entwurf konkrete Rechtsgrundlagen für die Verarbeitung personenbezogener Beschäftigtendaten enthalten wird.

Als Rechtsgrundlage kommt vor allem Art. 6 Abs. 1 lit. b DSGVO in Betracht. Die Vorschrift ist ähnlich wie § 26 Abs. 1 S. 1 BDSG formuliert. Nach Art. 6 Abs. 1 lit. b DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zu Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

d) § 26 BDSG ist im Übrigen weiterhin anwendbar

Der EuGH hat nur zu § 23 Abs. 1 S. 1 HDSIG (§ 26 Abs. 1 S. 1 BDSG) entschieden. Die übrigen Vorschriften des § 26 BDSG sind also weiterhin anwendbar. Es ist auch nicht davon auszugehen, dass die übrigen Vorschriften von § 26 BDSG für unanwendbar erklärt werden.[188] Die DSGVO nennt weder Anforderungen für die Verarbeitung personenbezogener Daten im Kontext der Aufdeckung und Verhinderung von Straftaten, noch stellt sie zusätzliche

---

[186] So etwa der HmbBfdI: https://perma.cc/DT7B-4MD2 (archiviert am 21.5.2023).

[187] S. dazu: *Wünschelbaum*, MMR-Aktuell 2023, 457188.

[188] *Ders.*, NZA 2023, 487, 544; i. E. auch: *Thüsing/Peisker*, NZA 2023, 213, 215.

Anforderungen an die Freiwilligkeit der Einwilligung im Beschäftigungskontext auf.[189] Auch auf die übrigen Vorschriften des § 26 BDSG hat das Urteil des EuGH keine Auswirkungen.[190] § 26 Abs. 3 S. 1 BDSG basiert auf Art. 9 Abs. 4 i. V. m. Abs. 2 lit. b DSGVO. § 26 Abs. 4 BDSG regelt, dass die Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen möglich ist. Vor dem Urteil des EuGH hatte § 26 Abs. 4 BDSG i. V. m. § 26 Abs. 1 S. 1 BDSG die klarstellende Bedeutung, dass eine Kollektivvereinbarung – insbesondere auch Betriebsvereinbarungen – eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sein kann. Dadurch, dass § 26 Abs. 1 S. 1 BDSG unanwendbar ist, hat § 26 Abs. 4 BDSG nicht mehr nur eine klarstellende Bedeutung, sondern ermächtigt die Kollektivpartner dazu, Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen. Schließlich ist § 26 Abs. 7 BDSG hinreichend spezifisch, indem die Datenverarbeitung auch auf manuelle Datenverarbeitungen ausgeweitet wird. Es gibt zudem keine Legaldefinition des Beschäftigtenbegriffs in der DSGVO, sodass die in § 26 Abs. 8 BDSG enthaltene Legaldefinition hinreichend spezifisch ist.[191]

2. Datenschutz im BetrVG

Gem. § 79a S. 1 BetrVG hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. § 79a S. 2 BetrVG weist die datenschutzrechtliche Verantwortlichkeit der Arbeitgeberin zu. Vor Einführung des § 79a BetrVG[192] war umstritten, wer Verantwortliche für die Datenverarbeitung ist, wenn personenbezogene Daten im Betrieb verarbeitet werden.[193] Auf die

---

[189] *Wünschelbaum*, NZA 2023, 487, 544.

[190] A. A. HBDI, Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023 Rs. C-34/21, S.5, https://perma.cc/6ZR6-RQ7F (archiviert am 10.6.2023), die ohne nähere Begründung davon ausgeht, dass auch die anderen Erlaubnistatbestände des § 23 HDSIG (§ 26 BDSG) in vielen Fällen unangewendet bleiben müssen.

[191] *Wünschelbaum*, NZA 2023, 487, 544.

[192] Einführung der Norm durch das Betriebsrätemodernisierungsgesetz v. 17.6.2021, BGBl. I S. 1762.

[193] ErfK/*Kania*, § 79a BetrVG Rn. 1; Richardi/*Thüsing*, § 79a BetrVG Rn. 1; *Flink*, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, 2020, S. 205 ff.

betriebsverfassungsrechtlichen Herausforderungen beim Einsatz algorithmischer Systeme wird in dieser Arbeit nicht näher eingegangen.[194]

3. Abgrenzung zum TMG/TKG/TTDSG

Das Telekommunikationsgesetz (TKG) reguliert gem. § 1 Abs. 1 TKG den Wettbewerb im Bereich der Telekommunikation und fördert leistungsfähige Telekommunikationsinfrastrukturen. Das Telemediengesetz (TMG) setzt die E-Commerce-Richtlinie [195] um und soll insbesondere die Dienstleistungsfreiheit durchsetzen.[196] Es gilt gem. § 1 Abs. 1 TMG für alle elektronischen Informations- und Kommunikationsdienste.

Bislang enthielten beide Gesetze Vorschriften zum Datenschutz in §§ 91 ff. TKG a. F. sowie §§ 11 ff. a. F. TMG. Am 1.12.2021 ist das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Dieses Bundesgesetz enthält spezifische Datenschutzvorschriften für Anbieter von Telekommunikationsdiensten und Telemediendiensten. Für den Untersuchungsgegenstand dieser Arbeit wird das TTDSG allerdings keine Rolle spielen, da der Anwendungsbereich sich auf Telekommunikations- und Telemediendienste beschränkt. Telekommunikationsdienste sind gem. § 2 Abs. 1 TTDSG i. V. m. § 3 Nr. 61 TKG „in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste". Bei einem Bewerbungsverfahren oder bei Entscheidungen im bestehenden Arbeitsverhältnis handelt es sich nicht um entgeltlich über das Telekommunikationsnetz erbrachte Dienste. Auch sind Fragen rund um das Fernmeldegeheimnis nach § 3 TTDSG oder Cookie-Vorgaben nach § 25 TTDSG für den Untersuchungsgegenstand irrelevant.[197]

---

[194] S. dazu ausführlich: *Blum*, People Analytics, 2021, S. 169 ff.; *Götz*, Big Data im Personalmanagement, 2020, S. 183 ff.

[195] RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr").

[196] MüKoBGB/*Martiny*, § 1 TMG Rn. 1.

[197] S. dazu: *Wünschelbaum*, NJW 2022, 1561.

D. Zwischenergebnis: Folgen für algorithmische Systeme

1. Datenschutzrechtliche Vorgaben gibt es sowohl im Unions- als auch im nationalen Recht. Im Anwendungsbereich des Unionsrechts sind die Grundrechte der GRCh maßgeblicher Prüfungsmaßstab. Ist das innerstaatliche Recht nicht vollständig durch Unionsrecht determiniert, dienen die nationalen Grundrechte als Prüfungsmaßstab.

2. Relevante Unionsgrundrechte sind in Art. 7, 8 GRCh verankert, die auch im Privatrechtsverhältnis berücksichtigt werden müssen, wenn die Vorschriften der DSGVO ausgelegt werden. [198] Zudem müssen die Vorgaben der EMRK bei der Auslegung der Unionsgrundrechte berücksichtigt werden.

3. Das Grundrecht auf Datenschutz nach Art. 7, 8 GRCh wird durch die DSGVO konkretisiert.

4. Die Vorgaben der DSGVO sind für algorithmische Systeme im Arbeitsrecht maßgeblich, wenn der Anwendungsbereich der DSGVO eröffnet ist. Da es sich bei den Ergebnissen des algorithmischen Systems häufig um Planungs- und Prognosedaten handelt, liegen personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO vor. Im Übrigen können maschinell lernende Systeme auch mit personenbezogenen Daten trainiert werden, sodass bereits der sachliche Anwendungsbereich der DSGVO eröffnet ist.[199] Persönlich wird es sich bei den betroffenen Personen immer um natürliche Personen handeln – auch in persönlicher Hinsicht ist der Anwendungsbereich eröffnet.[200] Der räumliche Anwendungsbereich ist sehr weit: Selbst wenn die Verarbeitung nicht in der Union stattfindet, das Unternehmen aber in der Union niedergelassen ist, ist die DSGVO anzuwenden.[201]

---

[198] S. Kapitel 5 A.II.2. (S. 60).
[199] Kapitel 6 B.IV. ff. (S. 133 ff.).
[200] Kapitel 5 A.III.2.b) (S. 70).
[201] Kapitel 5 A.III.2.c) (S. 70).

5. Art. 88 Abs. 1 DSGVO enthält eine Öffnungsklausel für den Beschäftigungskontext. Den Mitgliedstaaten steht im Beschäftigtendatenschutz eine autonome Regelungsbefugnis zu. Geht es um das konkrete Beschäftigungsverhältnis, war bislang § 26 Abs. 1 S. 1 BDSG die maßgebliche Vorschrift für die Verarbeitung personenbezogener Daten. Mit dem Urteil vom 30. März 2023[202] hat der EuGH entschieden, dass es sich bei § 26 Abs. S. 1 BDSG nicht um eine spezifischere Vorschrift i. S. d. Art. 88 Abs. 1 DSGVO handelt.[203] In der Konsequenz ist § 26 Abs. 1 S. 1 BDSG nicht weiter anwendbar.[204] Datenverarbeitungen im Beschäftigungskontext kann man deshalb nicht auf § 26 Abs. 1 S. 1 BDSG stützen.

6. Anforderungen an KI-Systeme wie z. B. Anforderungen an die Trainingsdaten stellt der KI-VO-KOM auf. Algorithmische Systeme, die im Bewerbungsverfahren oder laufenden Arbeitsverhältnis eingesetzt werden, werden von einer zukünftigen KI-VO erfasst sein.[205] Verarbeitet ein solches Hochrisiko-KI-System personenbezogene Daten, ist die zukünftige KI-VO neben der DSGVO anwendbar. Die Vorgaben für Hochrisiko-KI-Systeme nach dem KI-VO-KOM und die Frage, wie sich die Vorschriften der DSGVO und des KI-VO-KOM zueinander verhalten, werden im 4. Teil der Arbeit herausgearbeitet.[206]

---

[202] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[203] Kapitel 5 B.II.1. (S. 87).

[204] Kapitel 5 B.II.1.c) (S. 87).

[205] Kapitel 5 A.IV.5. (S. 82).

[206] S. Kapitel 10 (S. 341); Kapitel 11 (S. 363).

Kapitel 6

Rechtmäßigkeit der Datenverarbeitung

In diesem Kapitel wird untersucht, welche Voraussetzungen nach der DSGVO erfüllt sein müssen, damit es rechtmäßig ist, personenbezogene Daten mithilfe algorithmischer Systeme zu verarbeiten. Wie bereits erläutert worden ist, kann man die Datenverarbeitung im Beschäftigungskontext nicht länger auf § 26 Abs. S. 1 BDSG stützen. [1] Vielmehr sind auch die Rechtsgrundlagen des Art 6 DSGVO maßgeblich, wenn personenbezogene Daten im Beschäftigungskontext verarbeitet werden. Wenn es noch nicht um ein konkretes Beschäftigungsverhältnis geht, sind die Erlaubnistatbestände des Art. 6 DSGVO oder zusätzlich diejenigen des Art. 9 Abs. 2 DSGVO ohnehin einschlägig. Es handelt sich nicht um ein konkretes Beschäftigungsverhältnis, wenn (personenbezogene) Daten zu Trainingszwecken verarbeitet werden, damit das System auf unbekannte Daten angewendet werden kann. Werden die Ergebnisse tatsächlich verwendet, muss zusätzlich zur Rechtsgrundlage nach § 26 Abs. 2 BDSG, Art. 6 Abs. 1 DSGVO oder Art. 9 Abs. 2 DSGVO zudem Art. 22 DSGVO berücksichtigt werden.

Aufgrund der unterschiedlichen Vorschriften und der damit verbundenen unterschiedlichen Voraussetzungen ist es sinnvoll, bei Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch algorithmische Systeme zwischen den verschiedenen Verarbeitungsstadien zu differenzieren. Unterteilt wird zwischen dem Verarbeitungsstadium des Trainings, des Einsatzes algorithmischer Systeme sowie dem Stadiums, in dem das Ergebnis des Systems die Grundlage für Entscheidungen bildet.[2] Das erste Verarbeitungsstadium greift, wenn maschinell lernende Systeme erstellt werden, d. h. mit Trainingsdaten „gefüttert“ werden, um auf neue

---

[1] Kapitel 5 B.II.1. (S. 87).

[2] *Malorny*, JuS 2022, 289, 293 f.; *dies.*, RdA 2022, 170, 174.

unbekannte Daten angewendet werden zu können. [3] Im zweiten Verarbeitungsstadium geht es um den tatsächlichen Einsatz im Rahmen eines konkreten Beschäftigungsverhältnisses [4]: Daten konkreter Bewerber- oder Arbeitnehmerinnen werden erhoben und mithilfe des algorithmischen Systems verarbeitet. Das letzte Verarbeitungsstadium greift, wenn die Entscheidung, die mithilfe des algorithmischen Systems generiert wurde, tatsächlich durchgeführt wird. [5] Die Arbeitgeberinnen treffen ihre Entscheidung, der Bewerberin zu- oder abzusagen, auf Grundlage des Ergebnisses des algorithmischen Systems.

Bevor auf die einzelnen Verarbeitungsstadien eingegangen wird, müssen die generellen Anforderungen an die Rechtmäßigkeit [6] erläutert werden. Unabhängig von den spezifischen Vorgaben für die einzelnen Stadien gelten diese immer für die Datenverarbeitung.

A. Generelle Anforderungen an die Rechtmäßigkeit der Datenverarbeitung

Die DSGVO unterscheidet zwischen den Verantwortlichen (Art. 24 DSGVO), den gemeinsam Verantwortlichen (Art. 26 DSGVO) und der Auftragsverarbeiterin (Art. 28 DSGVO). Je nachdem ob eine Person Verantwortliche ist, ob es zwei gemeinsam Verantwortliche gibt oder ob eine Auftragsverarbeiterin involviert ist, müssen bestimmte Pflichten gewahrt werden.

Wird bei einer Arbeitgeberin ein algorithmisches System im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis von einer externen Dienstleisterin eingesetzt, muss geklärt sein, in welchem Verhältnis Arbeitgeberin und Dienstleisterin zueinander stehen. Je nachdem, ob sie

---

[3] Kapitel 6 B. (S. 117).
[4] Kapitel 6 C. (S. 161).
[5] Kapitel 6 D. (S. 204).
[6] Kapitel 6 A. (S. 98).

gemeinsame Verantwortliche sind oder ein Fall der Auftragsverarbeitung vorliegt, zieht das unterschiedliche Rechtsfolgen nach sich.

I. Verantwortlichkeit für die Datenverarbeitung

1. Datenschutzrechtlich Verantwortliche

Adressat der Verarbeitung personenbezogener Daten ist grundsätzlich die Verantwortliche. Das ist gem. Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Verantwortliche muss gem. Art. 24 DSGVO sicherstellen und nachweisen können, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Datenschutzrechtlich verantwortlich ist im Beschäftigungsverhältnis und im Bewerbungsverfahren zunächst die tatsächliche oder potenzielle Arbeitgeberin. Sie verarbeitet die personenbezogenen Daten und entscheidet über die Zwecke und Mittel der Verarbeitung personenbezogener Daten.

2. Einsatz von algorithmischen Systemen als Variante der der gemeinsamen Verantwortlichkeit oder der Auftragsverarbeitung

In den meisten Fällen werden algorithmische Systeme nicht vom Unternehmen selbst entwickelt werden, sondern das Unternehmen wird auf bereits entwickelte Systeme eines externen Dienstleisters zurückgreifen.[7] Das Verhältnis zwischen der verantwortlichen Arbeitgeberin und der externen Dienstleisterin kann je nach Ausgestaltung ein Auftragsverarbeitungsverhältnis sein oder aber sie sind gemeinsam für die Verarbeitung personenbezogener Daten verantwortlich.

a) Gemeinsame Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, sind sie „gemeinsam Verantwortliche“ (Art. 26 Abs. 1 S. 1 DSGVO). Wer für welche Phase der Verarbeitung verantwortlich

---

[7] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 23; *Kreutzer/Christiansen*, KI in Unternehmen, 2021, S. 16.

ist, muss in einer Vereinbarung (Art. 26 Abs. 1 S. 2 DSGVO) festgehalten werden. Diese Vereinbarung hat keine konstitutive Wirkung für die datenschutzrechtliche Verantwortlichkeit. [8] Von einer gemeinsamen Verantwortlichkeit wird man z. B. bei den einzelnen Unternehmen eines Konzerns ausgehen können. [9]

Ausschlaggebend ist, dass bei der gemeinsamen Verantwortlichkeit die Zwecke und Mittel der Verarbeitung von den Verantwortlichen gemeinsam festgelegt werden. Der Grad der Verantwortlichkeit muss dabei nicht zwingend gleich gelagert sein; es kann sein, dass die jeweiligen Verantwortlichen in unterschiedlichem Maß in die einzelnen Phasen der Verarbeitung mit einbezogen sind.[10] Die Anforderungen an die gemeinsame Verantwortlichkeit sind nicht besonders hoch: Es reicht aus, wenn die „eine Partei der anderen die Verarbeitung ermöglicht und damit faktischen Einfluss auf die Datenverarbeitung nimmt und der von der einen Partei verfolgte kommerzielle Zweck eine Gegenleistung für den der anderen Partei gebotenen Vorteil darstellt“ [11] . Möchte die Anbieterin des Systems die Daten der Arbeitgeberin nicht nur verarbeiten, sondern ihr maschinell lernendes System mit den Daten „weitertrainieren“, um es zu verbessern, sind Anbieterin des entsprechenden Systems und Arbeitgeberin gemeinsame Verantwortliche, wenn sie auch gemeinsame Mittel der Datenverarbeitung festlegen. Die Mittel der Datenverarbeitung meint die Techniken oder sonstigen Methoden, wie die personenbezogenen Daten verarbeitet werden sollen.[12] Die Arbeitgeberin und die Dienstleisterin verfolgen zwar unterschiedliche Zwecke: Der wirtschaftliche Vorteil der Arbeitgeberin liegt darin, dass sie zu verbesserten Ergebnissen in dem Bereich kommt, in dem das maschinell lernende System eingesetzt wird. Als Gegenleistung kann die Anbieterin des maschinell lernenden Systems mithilfe des Trainings mit den Daten das System weiter

---

[8] Gola/Heckmann/*Piltz*, Art. 26 DSGVO Rn. 20; *Piltz*, K&R, 709, 711.

[9] *Pötters*, Beschäftigtendatenschutz, 3. Aufl. 2021, § 15 B. II. 1. Rn. 22.

[10] EuGH, 29.7.2019 – C-40/17, NJW 2019, 2755, 2758 Rn. 70; zwar erging die Entscheidung noch zur RL 95/46, an der gemeinsamen Verantwortlichkeit hat sich jedoch mit dem Inkrafttreten der DSGVO nichts geändert. Insoweit können die Aussagen weiter herangezogen werden.

[11] EuGH, 29.7.2019 – C-40/17, NJW 2019, 2755, 2757 Rn. 69 ff.; *Ballestrem/Bär/Gausling u. a.* (Hrsg.), Künstliche Intelligenz, 2020, S. 24

[12] Gola/Heckmann/*Piltz*, Art. 26 DSGVO Rn. 13.

verbessern.[13] Es reicht aber aus, wenn die Zwecke eng miteinander verbunden sind oder sich ergänzen.[14] Der gegenseitige Nutzen von Zwecken kann ein Anhaltspunkt dafür sein, dass es sich um eine gemeinsame Verantwortlichkeit handelt.[15]

b) Auftragsverarbeitung

Auftragsverarbeiterin ist gem. Art. 4 Nr. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der Verantwortlichen verarbeitet. Kennzeichnendes Merkmal ist die Weisungsgebundenheit gegenüber der Verantwortlichen.[16] Die Auftragsverarbeiterin entscheidet grundsätzlich nicht über Zweck und Mittel der Verarbeitung. Trotzdem kann die Auftragsverarbeiterin gewisse Entscheidungsspielräume im Rahmen der Vorgaben der Verantwortlichen haben. Derartige Entscheidungsspielräume schließen die Auftragsverarbeitung nicht aus.[17] Entscheidende Kriterien sind etwa der Umfang des Weisungsrechts der Verantwortlichen, die Art und Weise wie gegenüber der betroffenen Person aufgetreten wird, in welchem Umfang und mit welchem Recht die Auftragsverarbeiterin oder die ihr unterstellen Personen kontrolliert werden, die Fachkompetenz der Beteiligten sowie die genaue Analyse der Handlungsspielräume.[18] Man ist insbesondere Verantwortliche, wenn man über die Zwecke der Datenverarbeitung entscheidet.[19]

Bei einem Auftragsverarbeitungsverhältnis muss ein Auftragsverarbeitungsvertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten gem. Art. 28 Abs. 3

---

[13] *Ballestrem/Bär/Gausling u. a.* (Hrsg.), Künstliche Intelligenz, 2020, S. 30.

[14] Gola/Heckmann/*Piltz*, Art. 26 DSGVO Rn. 12.

[15] Gola/Heckmann/*ders.*, Art. 26 DSGVO Rn. 12.

[16] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 22.

[17] *Datenschutzkonferenz* (DSK), Kurzpapier Nr. 13, 2018, S. 1.

[18] Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DSGVO Rn. 13.

[19] Kühling/Buchner/*ders.*, Art. 4 Nr. 7 DSGVO Rn. 13.

DSGVO geschlossen werden. Darin müssen u. a. Gegenstand, Dauer, Art und Zweck der Verarbeitung geregelt werden.

Erfolgt die Verarbeitung durch eine Auftragsverarbeiterin, darf die Verantwortliche nach Art. 28 Abs. 1 DSGVO nur mit einer Auftragsverarbeiterin zusammenarbeiten, die hinreichend Garantien dafür bietet, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO durchgeführt wird. Die Auftragsverarbeiterin darf nicht ohne Genehmigung oder allgemeine schriftliche Genehmigung der Verantwortlichen weitere Auftragsverarbeiterinnen hinzunehmen (Art. 28 Abs. 2 S. 1 DSGVO).

Verarbeitet die Arbeitgeberin die personenbezogenen Daten ihrer Arbeitnehmerinnen oder Bewerberinnen mithilfe des maschinell lernenden Systems einer externen Dienstleisterin, die die Daten nicht für eigene Zwecke weiterverarbeitet, liegt ein klassisches Auftragsverarbeitungsverhältnis vor.[20] Die Dienstleisterin wird die Daten im Rahmen der von der Auftraggeberin gemachten Vorgaben verarbeiten: Sie handelt nach den Weisungen der Auftraggeberin.[21]

c) Rechtsfolgen

Grundsätzlich müssen die Vorgaben der DSGVO eingehalten werden (Art. 26 und Art. 28 DSGVO). Dort sind die Pflichten für die gemeinsam Verantwortlichen und Auftragsverarbeiterinnen normiert.

Vorteil einer Auftragsverarbeitung ist, dass keine zusätzliche Rechtsgrundlage nach Art. 6 ff. DSGVO für die Verarbeitung benötigt wird.[22] Es reicht aus, dass die Verantwortliche die Datenverarbeitung selbst auf eine Rechtsgrundlage stützt.[23] Bei einer gemeinsamen Verantwortlichkeit muss für

---

[20] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, S. 28; vgl. *Joos*, NZA 2020, 1216, 1221.

[21] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, S. 28.

[22] *Datenschutzkonferenz* (DSK), Kurzpapier Nr. 13, 2018, S. 2.

[23] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 23; Sydow/Marsch/*Ingold*, Art. 28 DSGVO Rn. 31.

die weitergehende Datenverarbeitung durch die Anbieterin des Systems grundsätzlich eine geeignete Rechtsgrundlage vorliegen.[24] Etwas anderes gilt nur in dem Fall, wenn die Zwecke miteinander vereinbar sind gem. Art. 6 Abs. 4 DSGVO.[25]

Eine Auftragsverarbeiterin haftet gem. Art. 82 Abs. 2 S. 2 DSGVO für den durch eine Verarbeitung verursachten Schaden nur dann, wenn sie ihren speziell den Auftragsverarbeiterinnen auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen der für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Das ist anders bei einer gemeinsamen Verantwortlichkeit: Gem. Art. 82 Abs. 4 i. V. m. Abs. 2 S. 1 DSGVO haftet jede der gemeinsam Verantwortlichen im Falle einer nicht DSGVO-konformen Verarbeitung für den gesamten Schaden, sofern sie nicht ihr fehlendes Verschulden nachweisen kann, Art. 82 Abs. 3 DSGVO. Fehlt eine Vereinbarung nach Art. 26 DSGVO, können Bußgelder nach Art. 83 Abs. 4 lit. a DSGVO verhängt werden. Gleiches gilt bei Verstößen gegen Art. 28 DSGVO.

3. Benennung einer Datenschutzbeauftragten

Die Datenschutzbeauftrage unterstützt als interne Kontrollinstanz die Verantwortlichen und die Auftragsverarbeiterin, die Vorgaben der DSGVO einzuhalten. [26] Nach Art. 37 Abs. 1 DSGVO muss zwingend ein Datenschutzbeauftragter benannt werden, wenn die Verarbeitungsvorgänge eine regelmäßige und systemische Überwachung von betroffenen Personen erfordert (Art. 37 Abs. 1 lit. b DSGVO) oder besondere Kategorien personenbezogener Daten verarbeitet werden (Art. 37 Abs. 1 lit. c. DSGVO). Eine systemische Überwachung kann ggf. vorliegen, wenn im bestehenden Arbeitsverhältnis die Leistung der Arbeitnehmerinnen gemessen werden soll. Es ist nicht ausgeschlossen, dass im Bewerbungsverfahren oder bestehenden Arbeitsverhältnis besondere Kategorien personenbezogener Daten verarbeitet

---

[24] *Ballestrem/Bär/Gausling u. a.* (Hrsg.), Künstliche Intelligenz, 2020, S. 30.

[25] S. dazu unter: Kapitel 6 B.IV.1. (S. 133).

[26] Kühling/Buchner/*Bergt*, Art. 37 DSGVO Rn. 1.

werden, sodass eine Datenschutzbeauftragte ggf. bereits aus diesem Grund benannt werden muss.

Eine Datenschutzbeauftragte kann gem. Art. 37 Abs. 6 DSGVO eine Beschäftigte der Verantwortlichen oder der Auftragsverarbeiterin sein oder ihre Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen. Es besteht mithin die Wahlmöglichkeit, eine interne oder externe Datenschutzbeauftragte zu bestellen.[27] Voraussetzung für die Benennung als Datenschutzbeauftragte ist die berufliche Qualifikation und das Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis sowie die Fähigkeit, die in Art. 39 DSGVO genannten Aufgaben zu erfüllen (Art. 37 Abs. 5 DSGVO).

II. Erfordernis einer Rechtsgrundlage

Werden personenbezogene Daten verarbeitet, muss eine Rechtsgrundlage erfüllt sein. Zudem müssen die datenschutzrechtlichen Grundsätze in Art. 5 DSGVO berücksichtigt werden.[28]

1. Art. 6 DSGVO als zentrale Vorschrift

a) Überblick über Art. 6 DSGVO

Grundsätzlich ist die Verarbeitung personenbezogener Daten verboten, ggf. aber nach Art. 6 Abs. 1 S. 1 DSGVO zulässig (sog. Verbot mit Erlaubnisvorbehalt).[29] Die Zulässigkeitstatbestände für die die Verarbeitung personenbezogener Daten sind dort abschließend aufgelistet.[30] Demnach ist die Verarbeitung nur rechtmäßig, wenn

- eine Einwilligung der betroffenen Person vorliegt (Art. 6 Abs. 1 S. 1 lit. a DSGVO);

---

[27] Kühling/Buchner/*ders.*, Art. 37 DSGVO Rn. 36.

[28] Dazu sogleich unter: Kapitel 6 A.IV. (S. 133).

[29] *Aligbe*, Einstellungs- und Eignungsuntersuchungen, 2. Aufl. 2021, A. I. 4. Rn. 29; Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 2.

[30] Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 1.

- die Verarbeitung zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (Art. 6 Abs. 1 S. 1 lit. b DSGVO);
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung der Verantwortlichen erforderlich ist (Art. 6 Abs. 1 S. 1 lit. c DSGVO);
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 S. 1 lit. d DSGVO);
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Verantwortlichen übertragen wurde (Art. 6 Abs. 1 S. 1 lit. e DSGVO) oder
- die Verarbeitung zur Wahrung der berechtigten Interessen der Verantwortlichen oder einer Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Abs. 1 S. 1 lit. f DSGVO).

b) Art. 9 DSGVO als zusätzliche Voraussetzung neben Art. 6 DSGVO

Art. 9 DSGVO regelt die Verarbeitung besonderer Kategorien personenbezogener Daten („sensible Daten"). Gem. Art. 9 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten, aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Peron, untersagt.[31]

Art. 9 Abs. 2 DSGVO normiert Ausnahmetatbestände, unter denen solche Daten dennoch verarbeitet werden dürfen. Das Verhältnis von Art. 6 DSGVO zu Art. 9 DSGVO ist unklar: Einerseits könnte man Art. 9 DSGVO als *lex*

[31] S. zu unmittelbar und mittelbar sensiblen Daten etwa *Hacker*, Datenprivatrecht, 2020, S. 236 f.

specialis zu Art. 6 DSGVO einstufen.[32] Die Verarbeitung sensibler Daten würde sich allein nach Art. 9 DSGVO richten. Andererseits könnte man Art. 9 DSGVO so verstehen, dass er zusätzliche Vorgaben neben Art. 6 DSGVO schafft.[33] Neben den Voraussetzungen des Art. 6 DSGVO müssten bei besonderen Kategorien personenbezogener Daten auch die Voraussetzungen des Art. 9 DSGVO erfüllt sein, damit man die personenbezogenen Daten verarbeiten kann.

Der Wortlaut von Art. 6 und 9 DSGVO schließt ein „Nebeneinander" der Vorschriften nicht aus. Art. 6 DSGVO regelt – so steht es in der Überschrift – die Rechtmäßigkeit der Verarbeitung. Dabei differenziert Art. 6 DSGVO nicht zwischen der Verarbeitung verschiedener Arten personenbezogener Daten, sondern bezieht sich allgemein auf deren Verarbeitung. Aus Erwägungsgrund 51 S. 5 DSGVO ergibt sich, dass „zusätzlich zu den speziellen Anforderungen an eine [Verarbeitung besonderer Kategorien personenbezogener Daten] [...] die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung gelten [sollen]". Damit wird explizit auf Art. 6 DSGVO Bezug genommen, woraus man schließen könnte, dass bei einer Verarbeitung sensibler Daten sowohl die Voraussetzungen nach Art. 9 DSGVO als auch nach Art. 6 DSGVO erfüllt sein müssen. Das entspricht auch dem gesetzgeberischen Willen, nach dem neben einem Ausnahmetatbestand von Art. 9 Abs. 2 DSGVO „eine Rechtsgrundlage für die Verarbeitung nach Art. 6 Abs. 1 [DSGVO] [vorliegen muss]"[34]. Werden sensible Daten nach Art. 9 Abs. 1 DSGVO verarbeitet, ist eine Verarbeitung solcher Daten somit nur unter den *zusätzlichen* Voraussetzungen des Art. 9 Abs. 2 DSGVO zulässig.[35] Die Vorgaben des Art. 9 Abs. 2 DSGVO sind

---

[32] Gola/Heckmann/*Schulz*, Art. 9 Rn. 5; so wohl auch Ehmann/Selmayr/*Schiff*, Art. 9 DSGVO Rn. 10 f.; differenziert: BeckOK Datenschutzrecht/*Albers/Veit*, Art. 9 DSGVO Rn. 11.

[33] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 9 DSGVO Rn. 11; *Blum*, People Analytics, 2021, S. 141; NK-Datenschutzrecht/*Petri*, Art. 9 DSGVO Rn. 3; Kühling/Buchner/*Weichert*, Art. 9 DSGVO Rn. 4.

[34] *BT-Drs. 18/11325*, S. 94.

[35] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 9 DSGVO Rn. 11; *Blum*, People Analytics, 2021, S. 141.

allerdings strenger als die des Art. 6 DSGVO[36], weshalb die Voraussetzungen des Art. 6 Abs. 1 DSGVO regelmäßig erfüllt sind, wenn die Voraussetzungen nach Art. 9 Abs. 2 DSGVO vorliegen.

c) Sperrwirkung gegenüber Art. 6 Abs. 1 S. 1 lit. f DSGVO

Art. 9 DSGVO sperrt allerdings Art. 6 Abs. 1 S. 1 lit. f DSGVO: Art. 9 Abs. 2 DSGVO sieht keine für Art 6 Abs. 1 S. 1 lit. f. DSGVO vergleichbare Ausnahme vor. Art. 6 Abs. 1 S. 1 lit. f DSGVO kann als allgemeine Interessenabwägungsklausel [37] eine Vielzahl an Fällen erfassen. Die Verarbeitung sensibler Daten ist hingegen nur in bestimmten Fällen zulässig, die in Art. 9 Abs. 2 DSGVO geregelt sind. Würde man Art. 6 Abs. 1 S. 1 lit. f DSGVO als Rechtsgrundlage heranziehen, wenn man sensible Daten verarbeitet, würde das den eng gefassten Ausnahmen nach Art. 9 Abs. 2 DSGVO zuwiderlaufen. Art. 6 Abs. 1 S. 1 lit. f DSGVO scheidet mithin für die Verarbeitung sensibler Daten aus.[38]

d) Zweckänderung nach Art. 6 Abs. 4 DSGVO möglich

Art. 6 Abs. 4 DSGVO regelt die Verarbeitung zu einem anderen Zweck als demjenigen, zu dem die personenbezogenen Daten erhoben wurden.[39] Wie sich Art. 9 DSGVO zu Art. 6 Abs. 4 DSGVO verhält, lässt sich nicht ausdrücklich Art. 9 DSGVO entnehmen. Allerdings muss gem. Art. 6 Abs. 4 lit. c DSGVO „die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden" bei der Prüfung berücksichtigt werden, ob die Verarbeitung zu einem anderen Zweck mit demjenigen vereinbar ist, zu dem die personenbezogenen Daten ursprünglich erhoben wurden. Art. 6 Abs. 4 lit. c DSGVO setzt somit

---

[36] S. dazu auch: *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 100 f.

[37] Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 141.

[38] Gola/Heckmann/*Schulz*, Art. 9 DSGVO Rn. 5; *Hornung*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 91, 100.

[39] S. dazu auch unter: Kapitel 6 B.IV.1. (S. 133).

tatbestandlich voraus, dass auch Kategorien besonderer Personen einer Zweckänderung zugänglich sind.[40]

2. Art. 6 Abs. 1 S. 1 lit. b DSGVO als Rechtsgrundlage bei der Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis

a) § 26 Abs. 1 S. 1 BDSG als unanwendbare Vorschrift

§ 26 BDSG regelt die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses. Wie bereits ausgeführt worden ist, ist § 26 Abs. 1 S. 1 BDSG keine spezifischere Vorschrift i. S. d. Art. 88 Abs. 1 DSGVO und bleibt somit unangewendet.[41] Seit dem Urteil des EuGH vom 30. März 2023[42] kann man die Verarbeitung personenbezogener Daten im Beschäftigungskontext nicht mehr auf § 26 Abs. 1 S. 1 BDSG stützen. Als Rechtsgrundlage kommt vor allem Art. 6 Abs. 1 lit. b DSGVO in Betracht. Die Vorschrift ist ähnlich wie § 26 Abs. 1 S. 1 BDSG formuliert. Nach Art. 6 Abs. 1 lit. b DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.

b) Keine Sperrwirkung gegenüber den anderen Erlaubnistatbeständen des Art. 6 DSGVO

Der Anwendungsbereich des § 26 Abs. 1 BDSG ist auf „Zwecke des Beschäftigungsverhältnisses“ beschränkt. § 26 Abs. 1 BDSG ist seit dem Urteil des EuGH vom 30. März 2023[43] ohnehin nicht mehr anwendbar.[44] Man muss daher auch bei der Verarbeitung personenbezogener Daten hinsichtlich eines konkreten Beschäftigungsverhältnisses auf die Rechtsgrundlagen der DSGVO

---

[40] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 9 DSGVO Rn. 12; Gola/Heckmann/*Schulz*, Art. 9 DSGVO Rn. 7; a. A. Ehmann/Selmayr/*Schiff*, Art. 9 DSGVO Rn. 11.

[41] Kapitel 5 B.II.1.c) (S. 92).

[42] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[43] Kapitel 5 B.II.1.c) (S. 92).

[44] Kapitel 5 B.II.1.c) (S. 92).

zurückgreifen. Sollen Daten verarbeitet werden, die nicht unmittelbar für die Zwecke eines konkreten Beschäftigungsverhältnisses relevant sind, kann etwa auf Art. 6 Abs. 1 S. 1. lit. f DSGVO zurückgegriffen werden, sofern es sich nicht um sensible Daten nach Art. 9 Abs. 1 DSGVO handelt. Wann ein solcher Zweck vorliegt, ist einzelfallabhängig und wird nicht immer leicht zu bestimmen sein. Ein Beispiel, wann ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit. f DSGVO möglich ist, ist etwa die Verarbeitung von Beschäftigtendaten, wenn eine *Due Diligence* bei einem Unternehmenskauf durchgeführt wird oder es zu einem Betriebsübergang kommt. [45] In diesem Fall müssen die Daten verarbeitet werden, weil das Unternehmen geprüft wird, nicht aber, weil es um die Begründung, Durchführung oder Beendigung eines konkreten Beschäftigungsverhältnisses geht.

Für Einwilligungen ist § 26 Abs. 2 BDSG gegenüber Art. 6 Abs. 1 S. 1 lit. a DSGVO spezieller: Wann immer es somit um Einwilligungen geht, die das konkrete Beschäftigungsverhältnis betreffen, ist § 26 Abs. 2 BDSG maßgeblich. Für die grundsätzlichen Voraussetzungen sind aber weiterhin Art. 4 Nr. 11, 6 Abs. 1 lit. a sowie 7 DSGVO i. V. mit den Erwägungsgründen zu beachten.[46]

Eine Rechtsgrundlage für die Weiterverarbeitung zu anderen als den ursprünglich genannten Zwecken sieht § 26 BDSG nicht vor. Art. 6 Abs. 4 DSGVO ist insofern weiterhin anwendbar.[47]

c) § 26 Abs. 3 S. 1 BDSG als Umsetzung von Art. 9 Abs. 2 lit. b DSGVO

Der nationale Gesetzgeber hat mit § 26 Abs. 3 S. 1 BDSG die Regelungsbefugnis der Öffnungsklausel mit Art. 9 Abs. 2 lit. b DSGVO umgesetzt und geregelt, dass eine Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen

---

[45] *Kort*, NZA 2018, 1097, 1099.

[46] Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 62; Taeger/Gabel/*Zöll*, Rn. 75 ff.

[47] *Däubler*, Gläserne Belegschaften, 9. Aufl., § 5 Rn. 185.

Person am Ausschluss der Verarbeitung überwiegt. Eine Einwilligung ist ebenfalls möglich, wenn sie sich ausdrücklich auf die Daten nach Art. 9 Abs. 1 DSGVO bezieht, vgl. § 26 Abs. 3 S. 2 Hs. 2 BDSG. Nach § 26 Abs. 3 S. 2 Hs. 1 BDSG müssen zudem die Voraussetzungen nach § 26 Abs. 2 BDSG vorliegen. Hinzu kommen die Voraussetzungen des § 22 Abs. 2 DSGVO, die gem. § 26 Abs. 3 S. 3 BDSG entsprechend anzuwenden sind.

Für sich genommen ist § 26 Abs. 3 S. 1 BDSG kein eigener Erlaubnistatstand, da die Norm auf Rechte oder Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes verweist.[48] Es muss somit eine andere Norm vorliegen, um die Datenverarbeitung zu rechtfertigen. Eine Verpflichtung aus dem Arbeitsvertrag kann sich aber auch aus einer Kollektivvereinbarung ergeben.[49]

Werden sensible Daten durch algorithmische Systeme verarbeitet, ist somit § 26 Abs. 3 S. 1 BDSG einschlägig. Wie auch bei § 26 Abs. 1 S. 1 BDSG muss bei dieser Rechtsgrundlage eine Erforderlichkeitsprüfung durchgeführt werden. Der Maßstab ist aber gegenüber demjenigen in § 26 Abs. 1 S. 1 BDSG verschärft.[50]

III. Nebeneinander von Rechtfertigungstatbeständen: Verarbeitung nach Wegfall einer Rechtsgrundlage

Fraglich ist zudem, ob eine Verarbeitung gleichzeitig auf mehrere Erlaubnistatbestände gestützt werden kann. Relevant wird die Frage etwa, wenn eine Einwilligung gem. Art. 7 Abs. 1 DSGVO widerrufen wird, die Verarbeitung aber auch noch auf eine andere Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO gestützt werden kann. Häufig kommt aufgrund ihres großen Anwendungsbereichs die alternative Verarbeitungsgrundlage Art. 6 Abs. 1

---

[48] Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 40; Gola/Heckmann/*Pötters*, § 26 BDSG Rn. 76.

[49] Gola/Heckmann/*Pötters*, § 26 BDSG Rn. 76.

[50] Taeger/Gabel/*Zöll*, § 26 BDSG Rn. 87.

S. 1 lit. f DSGVO in Betracht, solange es sich nicht um sensible Daten nach Art. 9 Abs. 1 DSGVO handelt.[51]

1. Wortlaut von Art. 6 und 17 DSGVO

Die DSGVO verhält sich nicht ausdrücklich dazu, ob eine Verarbeitung gleichzeitig auf mehrere Rechtsgrundlagen gestützt werden kann. Der Wortlaut des Art. 6 Abs. 1 DSGVO sieht vor, dass „die Verarbeitung nur rechtmäßig ist, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist". Aus dem Wort *mindestens* kann man schlussfolgern, dass mehr als nur eine Rechtsgrundlage erfüllt sein kann. Auch sieht Art. 17 Abs. 1 lit. b DSGVO vor, dass die betroffene Person das Recht hat, die Löschung der personenbezogenen Daten zu verlangen, wenn sie ihre Einwilligung widerrufen hat und es an einer *anderweitigen* Rechtsgrundlage für die Verarbeitung fehlt. Auch diese Formulierung spricht dafür, dass es möglich sein muss, die Verarbeitung auf unterschiedliche Rechtsgrundlagen zu stützen.[52]

2. Ansichten in der Literatur und der Rechtsprechung

In der Literatur wird das Nebeneinander von Rechtsgrundlagen für möglich gehalten, teilweise aber mit unterschiedlichen Anforderungen.[53] *Blum* ist der Ansicht, dass die widerrufene Einwilligung – möchte man die weitere Verarbeitung auf Art. 6 Abs. 1 S. 1 lit. f DSGVO stützen – im Rahmen der Interessenabwägung zu berücksichtigen sei: Nur wenn trotz der widerrufenen Einwilligung die Interessen der Verantwortlichen gegenüber den Interessen der betroffenen Person überwiegen, dürften die Daten weiterverarbeitet werden.[54] Dem kann man aber entgegenhalten, dass an eine Datenverarbeitung, die ohne Einwilligung auch nach Art. 6 Abs. 1 S. 1 lit. f DSGVO zulässig wäre, nicht höhere Anforderungen gestellt werden sollten,

---

[51] S. Kapitel 6 A.II.1.c) (S. 107).

[52] *Krusche*, ZD 2020, 232, 235.

[53] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 25 f.; Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 22; *Bunnenberg*, JZ 2020, 1088, 45 f.

[54] *Blum*, People Analytics, 2021, S. 108; so auch Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 11.

wenn die Verantwortliche auch die Einwilligung der Betroffenen eingeholt hat.[55]

Götz zufolge ist das Nebeneinander von Einwilligung und anderer Rechtsgrundlage möglich, solange die Verantwortliche die betroffene Person informiert hat.[56] Das wird auch von *Schantz* so vertreten.[57]

Der EuGH geht in einer Entscheidung, die noch zur DSRL erging, darauf ein, dass mehrere Zulässigkeitsgründe nach Art. 6 DSRL erfüllt sind.[58] Er führt nicht näher aus, in welchem Verhältnis die Gründe zueinander stehen. Allein aber die Tatsache, dass mehrere Rechtsgrundlagen gleichzeitig erfüllt sind, führt im Umkehrschluss dazu, dass es möglich sein muss, auf mehrere Rechtsgrundlagen zurückgreifen zu können.

3. Ansicht der Art. 29-Datenschutzgruppe und des EDSA

Die Art. 29-Datenschutzgruppe ging in ihren Leitlinien, angenommen am 28. November 2017, davon aus, dass man bei einer widerrufenen Einwilligung die personenbezogenen Daten auf einer anderen Rechtsgrundlage weiterverarbeiten dürfe, solange man die betroffene Person gem. Art. 13, 14 DSGVO über die Änderung der Rechtsgrundlage informiere.[59] Gleichzeitig wurde in den Leitlinien aber auch ausgeführt, dass die Verantwortliche nicht rückwirkend Art. 6 Abs. 1 S. 1 lit. f DSGVO als Verarbeitungsgrundlage wählen kann, wenn Probleme mit der Gültigkeit der Einwilligung auftreten.[60] Die Aussagen der Art. 29-Datenschutzgruppe sind in dem Kontext mithin

---

[55] *Veil*, NJW 2018, 3337, 3342.

[56] *Götz*, Big Data im Personalmanagement, 2020, S. 55.

[57] NK-Datenschutzrecht/*Schantz*, Art. 6 DSGVO Rn. 12.

[58] EuGH, 9.3.2017 – C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce ./. Salvatore Manni,* juris, Rn. 41.

[59] *Art. 29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259), S. 27.

[60] *Dies.*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259), S. 28.

nicht konsistent. Der EDSA hat die Leitlinien übernommen, sodass die Ansicht weiterhin gilt.[61]

Auch die DSK ist dieser Ansicht: Es sei unzulässig, die Datenverarbeitung auf eine andere Rechtsgrundlage zu stützen, wenn die Einwilligung nicht mehr als Rechtsgrundlage herangezogen werden könne.[62]

4. Fazit: Nebeneinander von Rechtsgrundlagen möglich

Vor dem Hintergrund der genannten Argumente ist es überzeugend, dass auf eine andere Rechtsgrundlage zurückgegriffen werden kann, wenn die Einwilligung widerrufen wird und die Voraussetzungen der anderen Rechtsgrundlage bereits vor der Verarbeitung vorlagen.[63] Der Wortlaut von Art. 6 Abs. 1 und Art. 17 Abs. 1 lit. b DSGVO sprechen dafür, dass ein Nebeneinander von Rechtsgrundlagen möglich ist. Die Aussagen des EDSA sind hingegen nicht konsistent: Es kann nicht sein, dass nach Ansicht des EDSA einerseits die betroffene Person informiert werden muss, wenn eine Rechtsgrundlage geändert wird, etwa weil die Einwilligung widerrufen wird. Andererseits soll die Verantwortliche nicht von einer Einwilligung zu einer anderen Rechtsgrundlage wechseln.

Sofern die Voraussetzungen einer anderen Rechtsgrundlage vorliegen, sollte es der Verantwortlichen möglich sein, die Verarbeitung auf eine andere Rechtsgrundlage zu stützen. Zutreffend ist aber die Aussage des EDSA, dass die Person entsprechend informiert werden muss. Zwar sieht Art. 13 Abs. 1 lit. c DSGVO vor, dass die Person bei der *Erhebung* von personenbezogenen Daten über die Rechtsgrundlage informiert werden muss. Man könnte daraus schließen, dass Art. 13 Abs. 1 lit. c DSGVO nur für diese Art von Verarbeitung greift. Die Informationen gem. Art. 13, 14 DSGVO müssen der betroffenen Person zu Beginn des Datenverarbeitungsprozesses mitgeteilt

---

[61] Kapitel 5 A.III.1.b) (S. 63).

[62] *Datenschutzkonferenz* (DSK), Kurzpapier Nr. 20, S. 3.

[63] *Blum*, People Analytics, 2021, S. 108; *Kollmar/El-Auwad*, DSRITB 2020, 199, 209; im Ergebnis auch: *Krusche*, ZD 2020, 232, 237, der allerdings aufgrund der Ansicht der Art. 29-Datenschutzgruppe dazu rät, die Verarbeitung nur auf eine Rechtsgrundlage zu stützen; i. E. *Meinecke*, Datenschutz und Data Science, 2021, S. 160, der allerdings den Wechsel dann ausschließt, wenn die Einwilligung als einzige Rechtsgrundlage mitgeteilt wurde.

werden. Dieser beginnt mit der Erhebung der Daten, weshalb diese Verarbeitungsform auch explizit in Art. 13 Abs. 1 lit. c DSGVO genannt wird. Wird wegen eines Widerrufs der Einwilligung auf eine andere Rechtsgrundlage zurückgegriffen, muss diese Rechtsgrundlage entsprechend Art. 13 Abs. 1 lit. c DSGVO mitgeteilt werden. Die Erhebung ist eine Form der Verarbeitung gem. Art. 4 Nr. 2 DSGVO und ist nicht eingriffsintensiver als eine andere Verarbeitungsform, weshalb die Interessenlage vergleichbar und eine entsprechende Anwendung geboten ist. Jedenfalls ergibt sich aus Art. 5 Abs. 1 lit. a DSGVO, dass die Verarbeitung auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise vorgenommen wird. Dazu gehört auch, der Person die Rechtsgrundlage mitzuteilen.

IV. Verbindlichkeit der Datenschutzgrundsätze

Die in Art. 5 DSGVO aufgeführten Datenschutzgrundsätze enthalten Zielsetzungen für die Verarbeitung personenbezogener Daten.[64] Sie sind unmittelbar geltendes Recht und verbindlich: Gem. Art. 5 Abs. 1 DSGVO *müssen* personenbezogene Daten auf bestimmte Weise verarbeitet werden.[65]

Sie sind jedoch nur als „Grundsätze" und nicht als „Rechtmäßigkeitsvoraussetzungen" gekennzeichnet. Auf eine klare dogmatische Einordnung kommt es aber nicht an: Im Ergebnis ist relevant, dass bei einem Verstoß gegen die Grundsätze ein Bußgeld verhängt werden kann. Gem. Art. 83 Abs. 5 lit. a DSGVO können hohe Bußgelder von bis zu 20.000.000 EUR oder – im Fall eines Unternehmens – von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher Betrag höher ist.[66] Die Grundsätze müssen somit eingehalten werden.[67] Es kommt nicht darauf an, ob

---

[64] NK-Datenschutzrecht/*Roßnagel*, Art. 5 DSGVO Rn. 21.

[65] *Steege/Kuß*, in: Kuß/Steege/Chibanguza (Hrsg.), Künstliche Intelligenz, 2022, 1. Teil § 3 C. Datenschutzrecht Rn. 51; *Breyer*, DuD 2018, 311, 315; *Roßnagel*, ZD 2018, 339, 342.

[66] *Roßnagel*, ZD 2018, 339, 344; MHdb ArbR Band 1/*Wybitul*, § 96 BDSG Rn. 161.

[67] EuGH, 11.12.2019 – C-708/18, juris, Rn. 36.

sie als weitere *Rechtmäßig*keitsvoraussetzungen neben Art. 6 DSGVO treten oder lediglich als Grundsätze berücksichtigt werden müssen.

Für die konkrete Prüfung, ob die Verarbeitung personenbezogener Daten rechtmäßig ist, gibt es daher zwei Möglichkeiten: Man prüft zunächst die Rechtmäßigkeit nach Art. 6 DSGVO oder § 26 BDSG und danach, ob die Grundsätze nach Art. 5 DSGVO eingehalten wurden. Alternativ können sie bei abwägungsoffenen Erlaubnistatbeständen wie z. B. bei Art. 6 Abs. 1 S. 1 lit. f DSGVO im Rahmen der Abwägung schon bei der Prüfung der Rechtsgrundlage berücksichtigt werden. Bei der Erforderlichkeitsprüfung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO kann so die Einhaltung der Datenschutzgrundsätze eher für die Verarbeitung aufgrund berechtigter Interessen sprechen. Häufig sind genauere Ausprägungen der Grundsätze auch in anderen Vorschriften der DSGVO normiert. So sind etwa die Art. 13 ff. DSGVO eine Konkretisierung des Art. 5 Abs. 1 lit. a DSGVO.[68]

V. Zwischenergebnis: generelle Anforderungen an die Rechtmäßigkeit

1. Die Arbeitgeberin und die Anbieterin des algorithmischen Systems sind entweder gemeinsame Verantwortliche, oder es liegt ein Fall der Auftragsverarbeitung vor.[69] Je nachdem, welche Konstellation gegeben ist, greifen unterschiedliche Rechtsfolgen. Bei der Auftragsverarbeitung muss die Auftragsverarbeiterin keine Rechtsgrundlage für die weitere Verarbeitung vorweisen. Das ist bei der gemeinsamen Verantwortlichkeit anders: Für jede Verarbeitung muss eine geeignete Rechtsgrundlage vorliegen. Außerdem haftet die Auftragsverarbeiterin nur im Hinblick auf die speziell für das Auftragsverarbeitungsverhältnis vorgeschriebenen Pflichten oder wenn sie die Weisungen der Verantwortlichen missachtet hat.

2. Werden personenbezogene Daten verarbeitet, muss eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen. Werden sensible Daten verarbeitet, ist die Verarbeitung grundsätzlich nach

---

[68] Gola/Heckmann/*Franck*, Art. 13 DSGVO Rn. 2; s. zu §§ 13 ff. DSGVO: Kapitel 7 B (S. 246).

[69] Kapitel 6 A.I (S. 99).

Art. 9 Abs. 1 DSGVO verboten.[70] Unter den in Art. 9 Abs. 2 DSGVO genannten Ausnahmen ist eine Verarbeitung aber dennoch gestattet. Zusätzlich zu einer Ausnahme nach Art. 9 Abs. 2 DSGVO muss bei der Verarbeitung sensibler Daten aber auch eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen. Jedenfalls sperrt Art. 9 DSGVO Art. 6 Abs. 1 S. 1 lit. f DSGVO.[71] Art. 6 Abs. 4 DSGVO ist weiterhin anwendbar.[72]

3. Die DSGVO ist weiterhin in allen Bereichen anzuwenden, die § 26 BDSG nicht abschließend regelt. § 26 Abs. 1 S. 1 BDSG ist seit dem Urteil des EuGH vom 30. März 2023 nicht länger anwendbar.[73] Sollen Daten verarbeitet werden, die nicht unmittelbar für die Zwecke eines konkreten Beschäftigungsverhältnisses relevant sind, kann auf Art. 6 Abs. 1 S. 1 lit. f DSGVO zurückgegriffen werden, sofern es sich nicht um sensible Daten nach Art. 9 Abs. 1 DSGVO handelt. Werden sensible Daten während eines konkreten Beschäftigungsverhältnisses verarbeitet, ist § 26 Abs. 3 BDSG zu beachten. Werden personenbezogene Daten für ein konkretes Beschäftigungsverhältnis verarbeitet, ist statt bislang § 26 Abs. 1 S. 1 BDSG nun Art. 6 Abs 1 S. 1 lit. b DSGVO als Rechtsgrundlage heranzuziehen.[74]

4. Wird eine Einwilligung widerrufen, kann man die Verarbeitung auf eine andere Rechtsgrundlage stützen, sofern die Voraussetzungen der entsprechenden Rechtsgrundlage vorliegen.[75] Darüber muss man die betroffene Person aber zunächst informieren. Andernfalls verstößt die Verarbeitung jedenfalls gegen Art. 5 Abs. 1 lit. a DSGVO.

---

[70] Kapitel 6 A.II.1.b) (S. 105).
[71] Kapitel 6 A.II.1.c) (S. 107).
[72] Kapitel 6 A.II.1.d) (S. 107).
[73] S. dazu bereits unter: Kapitel 5 B.II.1.c) (S. 92).
[74] Kapitel 6 A.II.2. (S. 108).
[75] Kapitel 6 A.III. (S. 110).

5. Die Datenschutzgrundsätze nach Art. 5 DSGVO sind verbindlich und müssen eingehalten werden.[76]

B. Training maschinell lernender Systeme

Der folgende Abschnitt widmet sich den rechtlichen Anforderungen des Trainings[77] maschinell lernender Systeme. Zunächst wird der Frage nachgegangen, welche technischen und rechtlichen Herausforderungen sich beim Training mit anonymisierten Daten ergeben: Nachdem die technischen Möglichkeiten zur Anonymisierung vorgestellt wurden[78], wird die rechtliche Zulässigkeit der Anonymisierung[79] bewertet. Sodann wird die Möglichkeit untersucht, synthetische Daten zu verwenden[80]. Schließlich werden die Herausforderungen beim Training mit personenbezogenen Daten herausgearbeitet.[81] Als mögliche Rechtsgrundlage kommen Art. 6 Abs. 4 DSGVO, die Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO sowie Art. 6 Abs. 1 S. 1 lit. f DSGVO in Betracht. Auf die noch anwendbaren Vorgaben des § 26 BDSG[82] kommt es beim Training maschineller Systeme nicht an, weil es sich nicht um ein konkretes Beschäftigungsverhältnis handelt.[83]

---

[76] Kapitel 6 A.IV. (S. 114).
[77] S. dazu bereits unter: Kapitel 1 C. (S. 12).
[78] Kapitel 6 B.I. (S. 118).
[79] Kapitel 6 B.II.3. (S. 123).
[80] Kapitel 6 B.III. (S. 131).
[81] Kapitel 6 B.IV. (S. 133).
[82] Kapitel 5 B.II.1.d) (S. 92).
[83] S. dazu auch unter: Kapitel 6 C.I. (S. 161).

I. Technische Möglichkeiten zur Anonymisierung

Um personenbezogene Daten zu anonymisieren, werden i. d. R. zwei Techniken benutzt: Generalisierung und Randomisierung.[84]

1. Generalisierung

Bei der Generalisierung werden Datenbestände unter einem weniger spezifischen Wert zusammengefasst, sodass sie nicht mehr einer einzelnen Person, sondern nur noch einer Gruppe zugeordnet werden können.[85] Die Merkmale werden durch Veränderung der Größenskala oder -ordnung durch einen weniger spezifischen Wert ersetzt.[86] Etwa wird die Angabe einer Stadt bei einer Person durch eine Region ersetzt.[87] Die Anonymisierung ist erreicht, wenn anhand der Werte der einzelnen Merkmale kein Rückschluss mehr auf eine eindeutige Person gezogen werden kann.[88] Der Anwendungsbereich der DSGVO erstreckt sich nicht auf Personenmehrheiten oder -gruppen. Auch bei der Generalisierung gibt es verschiedene Techniken, um den Datensatz zu anonymisieren, auf die an dieser Stelle nicht im Detail eingegangen wird.[89]

Die Generalisierung ist aber in vielen Fällen keine ausreichende Methode, um personenbezogene Daten vollständig zu anonymisieren. Bei kleineren Gruppen ist es schwierig, die Daten so zu generalisieren, dass sie keinen

---

[84] *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 14; Jandt/Steidle/*Hammer*, B. IV. Rn. 289; NK-Datenschutzrecht/*Hansen*, Art. 4 Nr. 5 DSGVO Rn. 54; *Mühlenbeck*, Anonyme und pseudonyme Daten, 2022, S. 305 ff.; *Hölzel*, DuD 2018, 502, 505 f. unterscheidet hingegen zwischen perturbativen und nicht-perturbativen Methoden; s. zu weiteren technischen Vorgehensweise der Anonymisierung: *Kolain/Grafenauer/Ebers*, Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets Under the GDPR with a Special Focus on Smart Robotics, 2021, S. 15 ff.

[85] *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 19.

[86] *Dies.*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 19.

[87] *Dies.*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 19.

[88] Jandt/Steidle/*Hammer*, B. IV. Rn. 290.

[89] Zu den verschiedenen Techniken der Generalisierung s. *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 19 ff.

subjektiven Aussagehalt mehr haben. Kommt etwa nur eine Person aus einer bestimmten Region, wird auch die Sortierung nur nach Regionen als größere Einheit nicht helfen.[90] Werden mithin personenbezogene Daten bestimmter Arbeitnehmerinnen generalisiert, ist es abhängig von der Anzahl der Arbeitnehmerinnen, wie wirksam die Generalisierung ist. Aber auch bei größeren Gruppen ist die Generalisierung nicht unbedingt eine wirksame Methode zur Anonymisierung.[91] Je nach Verfügbarkeit von Informationen können auch bei größeren Datensätzen Rückschlüsse auf die personenbezogenen Daten hergestellt werden. So konnten Forscherinnen aufgrund von Metadaten deutscher Websites mit etwa 66 Millionen Nutzerinnen Rückschlüsse auf die aufgerufenen Seiten und auf die Verkettung der einzelnen Seitenaufrufe herstellen. Das wiederum ermöglichte die Nutzer zuzuordnen.[92]

2. Randomisierung

Bei der Randomisierung werden die zu der betroffenen Person gehörigen Daten verfälscht oder mit den Daten anderer betroffenen Personen aus dem Datensatz vertauscht.[93] So werden direkte Verbindungen zwischen Daten und betroffener Person entfernt.[94] Es wird aber gleichzeitig sichergestellt, dass – anders als bei der Generalisierung – statistische Verteilungen erhalten bleiben und weiterhin korrekte Ergebnisse mithilfe des Datensatzes geliefert werden.[95] Mögliche Techniken der Randomisierung wie stochastische Überlagerung, Vertauschung oder sog. *differential privacy* haben jedoch alle auch ihre Schwachstellen.[96] Bei allen Methoden kann es unter Umständen möglich sein, trotz der ergriffenen Maßnahmen Rückschlüsse auf die personenbezogenen Daten zu gewinnen. Wie hoch das Risiko für die betroffenen Personen ist, dass man aus den anonymisierten Daten dennoch auf die Person schließen kann,

---

[90] Vgl. dazu: *Götz*, Big Data im Personalmanagement, 2020, S. 77.

[91] Vgl. *Manthey*, Das datenschutzrechtliche Transparenzgebot, 2020, S. 292 ff.

[92] https://perma.cc/U52F-BUZ2 (archiviert am 27.01.2023).

[93] Jandt/Steidle/*Hammer*, B. IV. Rn. 289.

[94] *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 14.

[95] Jandt/Steidle/*Hammer*, B. IV. Rn. 289.

[96] *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 14 ff.; *Meinecke*, Datenschutz und Data Science, 2021, S. 286.

hängt davon ab, aus welchen verfügbaren (öffentlichen und nichtöffentlichen) Quellen man Zugang zu weiteren Informationen gewinnen kann.[97]

3. Anonymisierungstechniken bei Video-/Tonaufnahmen

Auch Bild- oder Videoaufnahmen können auf mehreren Wegen verändert und je nach Grad der Veränderung somit anonymisiert werden. Beispielsweise kann ein bestimmter Bildbereich aus dem Originalbild/-video herausgeschnitten werden, sodass ein Ausschnitt geschwärzt wird.[98] Andere Möglichkeiten sind die Verpixelung einzelner Bildausschnitte oder der Einsatz eines Kantenfilters, d. h., dass bei der Ursprungsaufnahme nur noch Kanten und Umrisse zu erkennen sind.[99] Auch können die Gesichtsmerkmale so verändert werden, dass quasi eine „andere" Person sichtbar ist („*deep natural anonymization*"[100]). Bei Tonaufnahmen können Passagen mit persönlichen Inhalten gelöscht und ersetzt werden und/oder die Tonhöhen verändert werden.[101]

Diese Anonymisierungstechniken haben aber zur Folge, dass es nicht mehr möglich ist, die Aufnahmen zu analysieren. Werden Gesichter und Stimmen unkenntlich gemacht oder derart verändert, dass sie stark vom Original abweichen, kann man sie nicht mehr im Hinblick auf Mimik und Intonation o. ä. analysieren.[102]

---

[97] *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 28.

[98] *Meyermann/Porzelt*, Hinweise zur Anonymisierung von qualitativen Daten, 2014, S. 12.

[99] *Bretthauer*, Intelligente Videoüberwachung, 2017, S. 62 ff.

[100] Diese Technik setzt *brighterAI* ein: https://perma.cc/JR6B-8TD4 (archiviert am 02.08.2022).

[101] *Meyermann/Porzelt*, Hinweise zur Anonymisierung von qualitativen Daten, 2014, S. 12.

[102] *Andersson/Sørvik*, FQS 2013, 1, 7 ; *Meyermann/Porzelt*, Hinweise zur Anonymisierung von qualitativen Daten, 2014, S. 12;

II. Ausschluss des Personenbezugs durch Anonymisierung

Bei anonymisierten Daten ist der Anwendungsbereich der DSGVO nicht eröffnet.[103] Gem. Erwägungsgrund 26 S. 3 DSGVO sollen die Grundsätze des Datenschutzes nicht für anonyme Daten gelten, d. h. in Fällen, in denen die betroffene Person nicht oder nicht mehr identifiziert werden kann. Eine Anonymisierung im Sinne der DSGVO liegt also vor, wenn der Personenbezug der Daten entfernt wurde.

1. Abgrenzung zur Pseudonymisierung

Im Unterschied zur Pseudonymisierung werden bei der Anonymisierung die Daten so verändert, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. [104] Gem. Art. 4 Nr. 5 DSGVO sind Daten pseudonymisiert, wenn sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Der Personenbezug kann nur mithilfe weiterer Informationen hergestellt werden. Man unterscheidet grundsätzlich drei Arten von Pseudonymen:[105] Die Betroffene nutzt ein selbst vergebenes Pseudonym, eine vertrauenswürdige Dritte vergibt ein Pseudonym, oder die für die Datenverarbeitung verantwortliche Stelle vergibt das Pseudonym.[106] Schreibt etwa eine Studentin ihre Klausur nicht unter der Angabe ihres Namens, sondern unter Angabe ihrer Prüfungsnummer, ist die Prüfungsnummer das Pseudonym für ihren Namen.

Das Ziel der Anonymisierung ist hingegen, dass der Personenbezug komplett aufgehoben wird.[107] Kann der Verarbeitungszweck auch mit anonymisierten Daten erreicht werden, kommt bei einer Verarbeitung nicht-anonymisierter Daten ein Verstoß gegen den Grundsatz der Datenminimierung gem. Art. 5

---

[103] S. zum Anwendungsbereich der DSGVO: Kapitel 5 A.III.2. (S. 65).

[104] S. Erwägungsgrund 26 S. 4 DSGVO; s. dazu auch: *Hacker*, Datenprivatrecht, 2020, S. 106.

[105] BeckOK Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 74 m.w.N.; zu technischen Anforderungen an Pseudonyme s. *Mühlenbeck*, Anonyme und pseudonyme Daten, 2022, S. 201 ff.

[106] BeckOK Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 74 ff.

[107] *Stürmer*, ZD 2020, 626, 627 ff.

Abs. 1 lit. c DSGVO in Betracht.[108] Nach diesem Grundsatz müssen die personenbezogenen Daten, die verarbeitet werden, für den Zweck angemessen und erheblich sowie auf das für den Zweck notwendige Maß beschränkt sein. Erheblich sind die Daten dann, wenn sie geeignet sind, den Zweck zu erreichen.[109] Die Daten sind angemessen, wenn sie dem Zweck uneingeschränkt zugeordnet werden können.[110] Werden personenbezogene Daten verarbeitet, obwohl es – auch in technischer Hinsicht – möglich gewesen wäre, sie zu anonymisieren, wäre die Verarbeitung nicht „auf das notwendige Maß beschränkt"[111].

2. Anonymisierende Wirkung der Pseudonymisierung

Erwägungsgrund 26 S. 2 DSGVO stellt klar, dass „einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, [...] als Informationen über eine identifizierbare natürliche Person betrachtet werden [sollten]". Pseudonymisierte Daten bleiben somit in aller Regel personenbezogene Daten.

Je nach Verarbeitungskontext können pseudonyme Daten auch anonymisierte Daten sein.[112] Das ist der Fall, wenn eine Re-Identifizierung nicht mehr möglich ist[113], wenn eine Dritte z. B. keinen Zugang mehr zu den entschlüsselnden Daten erhält. Das wiederum erfordert eine ständige Prüfung, ob nicht im Laufe der Zeit Zusatzwissen hinzugekommen ist, das eine Identifizierung der Person ermöglicht.[114] Insbesondere muss sichergestellt werden, dass die entschlüsselnden Daten besonders gesichert werden. Darf etwa eine Person, die für die Pseudonymisierung zuständig ist, den Schlüssel,

---

[108] *Götz*, Big Data im Personalmanagement, 2020, S. 76.

[109] BeckOK Datenschutzrecht/*Wolff*, Syst. A. Prinzipien des Datenschutzrechts Rn. 48.

[110] BeckOK Datenschutzrecht/*ders.*, Syst. A. Prinzipien des Datenschutzrechts Rn. 46.

[111] Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 58; vgl. Gola/Heckmann/*Pötters*, Art. 5 DSGVO Rn. 24.

[112] EuG, 26.4.2023 – T-557/20, juris, Rn. 101 ff.; *Gierschmann*, ZD 2021, 482, 483; *Roßnagel*, ZD 2018, 243, 245.

[113] *Art. 29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (WP 136), S. 21; *Roßnagel*, ZD 2018, 243, 244.

[114] *Roßnagel*, ZD 2018, 243, 247.

d. h. die zusätzlichen Informationen, die eine Identifizierung ermöglichen, aufbewahren, muss sie unbedingt sicherstellen, notwendige Garantien für den Schutz des Schlüssels bereitzustellen.[115]

3. Rechtliche Zulässigkeit der Anonymisierung

Werden personenbezogene Daten anonymisiert, werden nach überwiegender Ansicht[116] personenbezogene Daten i. S. d. Art. 4 Nr. 2 DSGVO verarbeitet, sodass eine Verarbeitungsgrundlage nach der DSGVO nötig ist. Diese Auffassung wird auch in dieser Arbeit zugrunde gelegt: Bevor personenbezogene Daten anonymisiert werden, sind sie personenbezogen und unterfallen dem Anwendungsbereich der DSGVO. Eine Verarbeitung personenbezogener Daten i. S. d. Art. 4 Nr. 2 DSGVO ist unter anderem auch das „Verändern" von Daten. Wird der Personenbezug entfernt, werden die personenbezogenen Daten verändert. Anders ist der Fall nur, wenn die Daten von vorneherein bereits anonym sind.

a) Art. 6 Abs. 1 S. 1. lit. f DSGVO

Neben der Möglichkeit einer Einwilligung wird insbesondere Art. 6 Abs. 1 S. 1 lit. f DSGVO relevant sein, um personenbezogene Daten zu anonymisieren. Willigt die Person ein, dass ihre Daten anonymisiert werden, sind die Voraussetzungen gegenüber einer Einwilligung bei der Verarbeitung personenbezogener Daten zu Trainingszwecken nicht anders.[117] Die Einwilligung als Rechtsgrundlage für die Anonymisierung wird an dieser Stelle nicht weiter vertieft, weil es für die Verantwortliche bei großen Datenmengen – die man in der Regel zu Trainingszwecken eines maschinell

---

[115] *Ders.*, ZD 2018, 243, 247.

[116] Gola/Heckmann/*Gola*, Art. 4 DSGVO Rn. 52; NK-Datenschutzrecht/*Hansen*, Art. 4 Nr. 5 DSGVO Rn. 23; *Hornung/Wagner*, ZD 2020, 223; *Der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit* (BfDI), Positionspapier zur Anonymisierung unter der DSGVO unter Berücksichtigung der TK-Branche, 2020, S. 5; *Gierschmann*, ZD 2021, 482, 485, die das Anonymisieren unter bestimmten Umständen mit dem Löschen gleichsetzt; a. A. *Thüsing/Rombey*, ZD 2021, 548.

[117] S. dazu unter: Kapitel 6 B.V. (S. 145).

lernenden Systems benötigt – kaum möglich sein wird, von jeder betroffenen Person die Einwilligung einzuholen, dass ihre Daten anonymisiert werden.[118]

Der Fokus liegt deshalb auf der Möglichkeit der Anonymisierung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO. Demnach ist die Anonymisierung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen der Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

aa) Anwendungsbereich

Gem. Art. 6 Abs. 2 DSGVO gilt Art. 6 Abs. 1 S. 1 lit. f. DSGVO nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Der Gesetzgeber schafft per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden. Der Behördenbegriff ist eng zu verstehen, sodass andere öffentliche Stellen von der Ausschlussklausel nicht betroffen sind.[119] Für den Untersuchungsgegenstand ist das indes nicht weiter relevant.

bb) Berechtigte Interessen

Das „berechtigte Interesse“ ist weit auszulegen.[120] Das Interesse umfasst all die Gründe, die eine Verantwortliche an der Verarbeitung haben kann oder den Nutzen, den die Verantwortliche aus der Verarbeitung zieht. [121] Grundsätzlich kommen rechtliche, wirtschaftliche oder ideelle Interessen als „berechtigte Interessen“ i. S. d. Vorschrift in Betracht. Bei einem Konzern kann gem. Erwägungsgrund 48 DSGVO ein berechtigtes Interesse darin liegen, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln.[122] Nach Erwägungsgrund 47 S. 2 DSGVO kann ein berechtigtes Interesse auch vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person

---

[118] Vgl. Braegelmann/Kaulartz/*Valkanova*, S. 337 Rn. 5.

[119] Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 24.

[120] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 68; Paal/Pauly/*Frenzel*, Art. 6 Rn. 27.

[121] *Art. 29-Datenschutzgruppe*, Stellungnahme 6/2014, S. 30 f.

[122] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 68.

und der Verantwortlichen besteht, z. B. wenn die betroffene Person Kundin der Verantwortlichen ist oder in ihren Diensten steht.

Die Interessen müssen im Einklang mit der Rechtsordnung stehen.[123] Mithin dient das Merkmal des „berechtigten Interesses" vor allem als Grobfilter legitimer Interessen.[124] Auch berechtigte Interessen Dritter werden berücksichtigt.[125] In Abgrenzung zu Art. 6 Abs. 1 S. 1 lit. e DSGVO werden öffentliche Interessen, die keinen Personenbezug aufweisen, nicht erfasst.[126]

Ziel der Anonymisierung ist es, den Personenbezug der Daten zu entfernen, um einen wirksamen Schutz für die Daten der betroffenen Person zu erzielen. Das ist ein legitimes Interesse i. S. d. Art. 6 Abs. 1 S. 1. lit. f DSGVO.

cc) Maßstab der Erforderlichkeit

Die Verarbeitung muss zur Wahrung des berechtigten Interesses erforderlich sein. Fraglich ist, welcher Maßstab zur Prüfung der Erforderlichkeit herangezogen wird.

Zum Teil wird die Auffassung vertreten, dass das Merkmal der Erforderlichkeit nicht als Ausprägung des Verhältnismäßigkeitsgrundsatzes zu verstehen sei.[127] Im Privatrechtsverkehr könne der strenge Verhältnismäßigkeitsgrundsatz nicht anzuwenden sein: Die Verhältnismäßigkeit sei ein Maßstab für das Handeln einer Hoheitsträgerin im Verhältnis zur Bürgerin.[128] Ein solches Verhältnis liege im Datenschutzrecht regelmäßig nicht vor, vielmehr handele es sich um ein Verhältnis zwischen der Verantwortlichen, die keine Hoheitsträgerin sei, und der Bürgerin.[129]

---

[123] *Herfurth*, ZD 2018, 514.

[124] NK-Datenschutzrecht/*Schantz*, Art. 6 DSGVO Rn. 98.

[125] NK-Datenschutzrecht/*ders.*, Art. 6 DSGVO Rn. 99.

[126] NK-Datenschutzrecht/*ders.*, Art. 6 DSGVO Rn. 99.

[127] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 69; Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 29.

[128] Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 29.

[129] Vgl. BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 69; Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 29.

Das überzeugt nicht. Auch wenn Reichweite, Umfang und Grenzen einer „mittelbaren Drittwirkung" der Grundrechte im Einzelnen unklar sind, sind Art. 7, 8 GRCh zu berücksichtigen, wenn die DSGVO ausgelegt wird.[130] Anhaltspunkte dafür, dass sich hinter dem Merkmal der Erforderlichkeit der Grundsatz der Verhältnismäßigkeit verbirgt, liefert Erwägungsgrund 39 S. 9 DSGVO. Demnach sollten personenbezogene Daten nur verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Der Verweis auf „andere Mittel" deutet auf eine Prüfung der Erforderlichkeit im engeren Sinn hin. Schließlich gebietet der in Art. 19 EUV normierte Grundsatz der Einheit der Rechtsordnung, dass das Tatbestandsmerkmal der Erforderlichkeit als Ausprägung des Verhältnismäßigkeitsgrundsatzes auszulegen ist.[131]

Erforderlich i. S. d. Art. 6 Abs. 1 S. 1 lit. f DSGVO ist die Verarbeitung mithin dann, wenn kein milderes, gleich effektives Mittel herangezogen werden kann. [132] Die Angemessenheitsprüfung ist nicht vom Merkmal der Erforderlichkeit bestimmt, weil Art. 6 Abs. 1 S. 1 lit. f DSGVO eine solche Abwägung bereits im Wortlaut vorsieht: Die Verarbeitung muss erforderlich sein, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen". Die Interessenabwägung ist in einem zweiten Schritt zu prüfen.

dd) Erforderlichkeit und entgegenstehende Interessen

Gegenüber der Anonymisierung gibt es kein gleich geeignetes, milderes Mittel, um den Personenbezug vollständig zu entfernen. Insbesondere ist die Pseudonymisierung kein milderes Mittel, weil der Personenbezug wiederhergestellt werden kann.[133] Auch wenn man die Daten löscht, ist das kein gleich geeignetes, milderes Mittel, weil die Daten nicht mehr verarbeitet

---

[130] Kapitel 5 A.II.1.b) (S. 58).

[131] Vgl. Calliess/Ruffert/*Wegener*, Art. 19 EUV Rn. 55.

[132] Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 147a; i. E. so auch: Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 20; i. E. auch *Blum*, People Analytics, 2021, S. 118; *Meinecke*, Datenschutz und Data Science, 2021, S. 178; *Herfurth*, ZD 2018, 514, 515 *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 218

[133] S. dazu bereits unter: Kapitel 6 B.II.1. (S. 121).

werden können.[134] Die Erforderlichkeit ist mithin bei der Anonymisierung personenbezogener Daten unproblematisch.

Im Hinblick auf die entgegenstehenden Interessen könnte man argumentieren, dass die betroffene Person der Anonymisierung offen gegenüberstehen dürfte, da ihre personenbezogenen Daten so besser geschützt werden. Bei einer wirksamen Anonymisierung ist eine Re-Identifizierung ausgeschlossen. Die Person dürfte kein entgegenstehendes Interesse haben.

Auf der anderen Seite hat die betroffene Person gem. Art. 7, 8 GRCh und auch auf nationaler Ebene aufgrund ihres Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG das Recht, dass ihre Daten gar nicht verarbeitet und im Zweifel eher gelöscht als anonymisiert werden.[135]

Allerdings müssen die Interessen der Person gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO *überwiegen*, also deutlich gewichtiger als die Interessen der Verantwortlichen eingestuft werden. Wenn eine wirksame Anonymisierung möglich ist, also eine Re-Identifizierung ausgeschlossen ist, muss das Interesse der betroffenen Person, dass ihre Daten gar nicht verarbeitet werden, hinter dem Interesse der Verantwortlichen, die Daten in anonymisierter Form zu verarbeiten, zurücktreten. Bei einer wirksamen Anonymisierung bestehen keine Risiken mehr für die betroffene Person.

b) Rechtsgrundlage für die Verarbeitung sensibler Daten

Für die Anonymisierung personenbezogener Daten stellt sich aber folgendes Problem: Art. 6 Abs. 1 S. 1 lit. f DSGVO ist keine Rechtsgrundlage für die Verarbeitung sensibler Daten nach Art. 9 Abs. 1 DSGVO.[136] Die Erlaubnistatbestände, die Art. 9 Abs. 2 DSGVO für die Verarbeitung vorsieht, werden für die Anonymisierung personenbezogener Daten zu Trainingszwecken – abgesehen von einer möglichen Einwilligung nach Art. 9

---

[134] S. dazu sogleich unter: Kapitel 6 B.II.3.c) (S. 129).

[135] *Hornung/Wagner*, ZD 2020, 223, 225; vgl. *Storms*, Datenschutz in der Unternehmenstransaktion, 2021, S. 200.

[136] Kapitel 6 A.II.1.c) (S. 107).

Abs. 2 lit. a DSGVO – nicht einschlägig sein:[137] Die Anonymisierung von Daten für Trainingszwecke eines maschinell lernenden Systems wird nicht erforderlich sein, damit die Verantwortliche oder die betroffene Person, die ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben darf (Art. 9 Abs. 2 lit. b DSGVO). Auch wird die Anonymisierung zu Trainingszwecken in Hinblick auf den zum Schutz *lebenswichtiger* Interessen der betroffenen Person nicht erforderlich sein (Art. 9 Abs. 2 lit. c DSGVO). Auch die anderen Rechtsgrundlagen nach Art. 9 Abs. 2 DSGVO sind inhaltlich nicht einschlägig.

Das führt dazu, dass die Anforderungen an die Anonymisierung sensibler Daten weitaus höher sind als die Anonymisierung sonstiger personenbezogener Daten. *Hornung* und *Wagner* sind der Auffassung, dass das grundsätzliche Verarbeitungsverbot für sensible Daten zu einem erhöhten Risiko für die Rechte der betroffenen Personen führe, was der Zielsetzung von Art. 9 Abs. 1 DSGVO widerspreche[138]: Es sei nachvollziehbar, die Verarbeitung sensibler Daten besonders zu schützen, wenn mit der Verarbeitung ein höheres Risiko für die Rechte der betroffenen Personen einhergehe. Nicht überzeugend sei es aber, erhöhte Anforderungen an die Verarbeitung sensibler Daten zu stellen, wenn die Rechte der betroffenen Personen durch die Verarbeitung stärker geschützt würden. Daher sei Art. 9 Abs. 1 DSGVO teleologisch zu reduzieren, wenn sensible Daten anonymisiert, gelöscht oder vernichtet werden sollten:[139] So könne man im Ergebnis Art. 6 Abs. 1 S. 1 lit. f DSGVO auch als Rechtsgrundlage für das Anonymisieren personenbezogener Daten heranziehen.

Dieser Vorschlag überzeugt aber nicht: Das Anonymisieren, Löschen und Vernichten von Daten sind unterschiedliche Verarbeitungsformen, die mit unterschiedlichen Risiken für die personenbezogenen Daten der betroffenen Personen einhergehen. Während Daten nicht mehr weiterverarbeitet werden, wenn sie gelöscht oder vernichtet worden sind, zielt die Anonymisierung hingegen darauf ab, dass man die Daten zu bestimmten Zwecken (weiter-

[137] *Hornung/Wagner*, ZD 2020, 223, 226.
[138] *Dies.*, ZD 2020, 223, 228.
[139] *Dies.*, ZD 2020, 223, 228.

)verarbeitet. Werden Daten anonymisiert, können – wie bereits ausgeführt[140] – ggf. Risiken für die ehemals personenbezogenen Daten bestehen.

Eine Anonymisierung sensibler Daten ist somit nur unter den zusätzlichen Voraussetzungen des Art. 9 Abs. 2 DSGVO möglich.

c) Art. 6 Abs. 1 S. 1 lit. c DSGVO i. V. m. Art. 17 DSGVO

Als mögliche Rechtsgrundlage für die Anonymisierung kann auch Art. 6 Abs. 1 S. 1 lit. c i. V. m. 17 DSGVO dienen, sofern die Löschung personenbezogener Daten mit der Anonymisierung gleichgesetzt werden kann. In Art. 17 Abs. 1 DSGVO ist das Recht der betroffenen Person geregelt, dass die Verantwortliche ihre personenbezogenen Daten löscht. In dogmatischer Hinsicht wird die Pflicht zur Anonymisierung dann analog zu Art. 17 Abs. 1 DSGVO als „rechtliche Verpflichtung, der die Verantwortliche unterliegt" i. S. d. Art. 6 Abs. 1 S. 1 lit. c DSGVO eingeordnet.

Die DSGVO definiert selbst nicht, was unter Löschung zu verstehen ist. In einem Urteil vom 20. Dezember 2017 [141] führte der EuGH zur Vorgängervorschrift von Art. 17 DSGVO zwar aus, dass das Recht auf Löschung einer Prüfungsarbeit bedeute, dass die Arbeit „zerstört" werde.[142] Daraus kann aber nicht allgemein geschlossen werden, dass ein Löschen auch das Vernichten beinhaltet.[143] Das Vernichten ist neben dem Löschen in Art. 4 Nr. 2 DSGVO als alternative Verarbeitungsform der Daten aufgeführt. Daher muss es einen Unterschied zwischen Löschen und Vernichten geben. Beim Löschen muss derart auf die Daten eingewirkt werden, dass „eine in den Daten verkörperte Information nicht mehr im üblichen Verfahren aus den verarbeiteten Daten ohne unverhältnismäßigen Aufwand gewonnen werden kann" [144]. Im Prinzip werden die Daten beim Löschen „unkenntlich"

---

[140] Kapitel 6 B.I. (S. 118).

[141] EuGH, 20.12.2017 – C-434/16, NJW 2018, 767.

[142] EuGH, 20.12.2017 – C-434/16, NJW 2018, 767, 769.

[143] Ehmann/Selmayr/*Kamann/Braun*, Art. 17 DSGVO Rn. 34 m. w. N.

[144] Ehmann/Selmayr/*dies.*, Art. 17 DSGVO Rn. 34; vgl. Gola/Heckmann/*Nolte/Werkmeister*, Art. 17 DSGVO Rn. 10; Kühling/Buchner/*Herbst*, Art. 17 DSGVO Rn. 37.

gemacht.[145] Werden Daten vernichtet, muss der Datenträger physisch beseitigt werden.[146]

Die DSGVO regelt nicht, ob Löschung und Anonymisierung personenbezogener Daten gleichgesetzt werden können. Systematisch betrachtet ist Art. 17 Abs. 1 DSGVO ein Betroffenenrecht: Unter bestimmten Voraussetzungen kann die betroffene Person von der Verantwortlichen verlangen, dass ihre personenbezogenen Daten gelöscht werden. Art. 17 Abs. 1 DSGVO setzt mithin ein Begehren der betroffenen Person voraus. Ein solches Begehren fehlt in vielen Szenarien, in denen Daten anonymisiert werden sollen. [147] Eine betroffene Person wird wohl kaum von der Verantwortlichen verlangen, dass ihre Daten gelöscht werden. Bei der Frage, ob man Löschen und Anonymisieren gleichsetzt, muss man vor allem das Risiko für die betroffene Person berücksichtigen. Der Zweck einer Anonymisierung und einer Löschung ist zumeist unterschiedlich: Das Ziel einer Anonymisierung ist, die Daten zu (anderen) Zwecken weiterzuverwenden.[148] Ziel einer Löschung der Daten ist hingegen, sie nicht mehr weiterzuverwenden.[149] Kann man allerdings die anonymisierten Daten nicht re-identifizieren, ist eine Anonymisierung eine Alternative zur Löschung der Daten.[150] Das stellt auch der EDSA in seinen Leitlinien 4/2019 zu Art. 25 DSGVO fest:[151] „Anonymization of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of reidentification, are regularly assessed."[152] Art. 6 Abs. 1 S. 1 lit. c i. V. m. 17 DSGVO ist somit eine taugliche Rechtsgrundlage, um personenbezogene Daten zu anonymisieren, solange eine Re-Identifikation bei den anonymisierten Daten ausgeschlossen ist.

---

[145] Ehmann/Selmayr/*Kamann/Braun*, Art. 17 DSGVO Rn. 34.
[146] *Roßnagel*, ZD 2021, 188, 189.
[147] *Hornung/Wagner*, ZD 2020, 223, 226.
[148] *Roßnagel*, ZD 2021, 188, 192.
[149] *Ders.*, ZD 2021, 188.
[150] *Eickstädt/Weaver*, DSRITB 2020, 287, 298; *Stürmer*, ZD 2020, 626-631, 630 ff.
[151] *Der Europäische Datenschutzausschuss* (EDSA), Guidelines 4/2019 on Article 25, 2020.
[152] *Ders.*, Guidelines 4/2019 on Article 25, 2020, S. 13.

4. Zwischenergebnis: wirksame Anonymisierung schwierig umsetzbar

1. Die Ausführungen zeigen, dass es technisch schwierig ist, aus einem umfassenden personenbezogenen Datenbestand einen vollständig anonymen Datenbestand zu generieren.[153] Der Anwendungsbereich der DSGVO ist aber nur dann nicht für anonyme Daten eröffnet, wenn die Daten auch wirksam anonymisiert sind, also der Personenbezug komplett aufgehoben und keine Re-Identifizierung mehr möglich ist.

2. Der Vorgang des Anonymisierens selbst ist eine Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO, sodass eine Rechtsgrundlage dafür vorliegen muss. [154] Sensible Daten können nur unter den zusätzlichen Voraussetzungen des Art. 9 Abs. 2 DSGVO anonymisiert werden.

3. Die Verantwortliche muss prüfen und dokumentieren, ob eine Anonymisierung technisch möglich ist. Ist sie technisch möglich, muss die Verantwortliche anonymisierte Daten verwenden, da sonst ein Verstoß gegen den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO vorliegt.

III. Synthetische Daten als Alternative zur Anonymisierung

Um dem Anwendungsbereich der DSGVO zu entgehen, ist es auch möglich, synthetische Daten für das Training des maschinell lernenden Systems zu verwenden. Synthetische Daten sind eine künstliche Repräsentation eines Originaldatensatzes. [155] Es ist technisch möglich, alle Datenarten zu synthetisieren, also auch Bilddateien. [156] Gegenüber echten Daten haben sie einige Vorteile:[157] Sie können unbegrenzt produziert werden.

---

[153] Vgl. *Winter/Battis/Halvani*, ZD 2019, 489; *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 5; s. dazu auch: *Ohm*, UCLA Law Rev. 2010, 1701.

[154] Kapitel 6 B.II.3. (S. 123).

[155] Braegelmann/Kaulartz/*Paal*, S. 439.

[156] *Drechsler/Jentsch*, Synthetische Daten, 2018, S. 6.

[157] *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, S. 132; *BT-Drs. 488/1/21*, S. 17 f.

Außerdem kann man bei der Erstellung künstlicher Daten besonders darauf achten, dass ein möglichst repräsentativer Datensatz entsteht.

Um synthetische Daten überhaupt generieren zu können, benötigt man je nach Art der Daten häufig eine entsprechende Anzahl personenbezogener Daten. Damit man die entsprechenden personenbezogenen Daten verarbeiten kann, um die synthetischen Daten zu generieren, benötigt man also eine Rechtsgrundlage gem. Art. 6 oder Art. 9 DSGVO.[158] Die Probleme, die sich bei der Anonymisierung ergeben, stellen sich somit auch bei der Generierung synthetischer Daten – sie verlagern sich nur an eine andere Stelle.[159]

Hinzu kommt, dass synthetische Daten im Ergebnis womöglich weiterhin personenbezogenen sind: Das hängt davon ab, wie stark sie dem Originaldatensatz gleichen.[160] Fraglich ist insoweit, ob die Verarbeitung synthetischer Daten in Einklang mit dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO steht: Anders als bei der Anonymisierung werden bei synthetischen Daten *neue* Daten generiert. Bei der Anonymisierung hingegen wird bei *vorhandenen* Daten der Personenbezug entfernt. Der Grundsatz der Datenminimierung greift aber nicht mehr, sofern synthetischen Daten der Personenbezug fehlt. Im Ergebnis muss für die Nutzung von synthetischen Daten vor diesem Hintergrund das Gleiche gelten wie für anonymisierte Daten: Wenn synthetische Daten wie auch anonymisierte Daten keinen Personenbezug aufweisen, gibt es keinen Grund, ihre Verarbeitung aus Gründen des Datenschutzes einzuschränken. Im Vorhinein muss aber sichergestellt werden, dass die Generierung der synthetischen Daten aus vorhandenen personenbezogenen Daten datenschutzrechtlich zulässig ist.

---

[158] Braegelmann/Kaulartz/*Meents*, S. 458 Rn. 49.

[159] *Rostalski*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 251, 258.

[160] Braegelmann/Kaulartz/*Kaulartz*, S. 470; a. A. *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 57.

IV. Training maschinell lernender Systeme als Zweckänderung gem. Art. 6 Abs. 4 DSGVO

Handelt es sich bei den Trainingsdaten um personenbezogene Daten i. S. d. Art. 4 Nr. 1 DSGVO, muss eine Rechtsgrundlage für die Verarbeitung vorliegen. Möchte eine Anbieterin eines maschinell lernenden Systems ihr System mit Daten trainieren, die ursprünglich zu einem anderen Zweck erhoben wurden, greift womöglich Art. 6 Abs. 4 DSGVO ein. Dieser trifft im Wesentlichen zwei Grundaussagen: Bei inkompatiblen Zwecken – also wenn der ursprüngliche und der neue Zweck nach der Kompatibilitätsprüfung des Art. 6 Abs. 4 DSGVO nicht miteinander vereinbar sind– dürfen Daten verarbeitet werden, wenn eine Einwilligung oder eine Verarbeitung nach Art. 6 Abs. 1 lit. c und e DSGVO vorliegt. Daten dürfen jedoch für einen anderen als den ursprünglich vereinbarten Zweck verarbeitet werden, wenn der neue und der ursprüngliche Zweck miteinander „vereinbar" sind. Dabei müssen die Kriterien nach Art. 6 Abs. 4 lit. a-e DSGVO erfüllt sein. Umstritten ist, ob bei der Weiterverarbeitung zu einem neuen Zweck, bei dem die Kriterien nach Art. 6 Abs. 4 DSGVO erfüllt sind, zusätzlich eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO erforderlich ist oder ob es sich bei Art. 6 Abs. 4 DSGVO um eine eigenständige Rechtsgrundlage handelt.

1. Art. 6 Abs. 4 DSGVO als eigenständige Rechtsgrundlage

Stimmen in der Literatur sprechen sich insbesondere mit Verweis auf Wortlaut und Systematik des Art. 6 DSGVO dafür aus, dass neben den Voraussetzungen nach Art. 6 Abs. 4 DSGVO noch eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO erforderlich sei: [161] Grundsätzlich sehe Art. 6 Abs. 1 DSGVO vor, dass die Verarbeitung „nur" rechtmäßig sei, wenn mindestens eine der nachstehenden Bedingungen erfüllt sei.[162] Eine in Art. 6 Abs. 1 DSGVO genannte Rechtsgrundlage müsse immer vorliegen, andernfalls sei die Verarbeitung rechtswidrig. [163] Aus der systematischen

---

[161] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 108; Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 19; *Blum*, People Analytics, 2021, S. 231; *Götz*, Big Data im Personalmanagement, 2020, S. 128; *Hacker*, Law, Innovation and Technology 13 (2021), 257, 275; *Meinecke*, Datenschutz und Data Science, 2021, S. 210.

[162] Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 183.

[163] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 108.

Stellung des Art. 6 Abs. 4 DSGVO ergebe sich, dass die in Abs. 1 genannte Rechtsgrundlage zusätzlich vorliegen müsse.[164] Art. 6 Abs. 1 DSGVO führe die Erlaubnistatbestände abschließend auf. Wenn der Gesetzgeber gewollt hätte, dass Art. 6 Abs. 4 DSGVO als eigener Erlaubnistatbestand gilt, hätte er ihn in Abs. 1 nennen müssen. Würde man keine gesonderte Rechtsgrundlage fordern, habe das zur Folge, dass die Rechtsgrundlage für die ursprüngliche Datenverarbeitung Legimitationsgrundlage für die weitere Datenverarbeitung sei, wenn die Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO positiv ausfalle.[165] Das sei unzureichend und entspreche nicht Art. 6 Abs. 1 DSGVO, der für jede Verarbeitung – mithin auch jede *Weiter*verarbeitung – eine Rechtsgrundlage fordere.[166]

Überzeugend ist es aber, das Erfordernis einer zusätzlichen Rechtsgrundlage abzulehnen.[167] Art. 6 Abs. 4 DSGVO ist so zu verstehen, dass für eine zweckändernde Weiterverarbeitung keine eigene Rechtsgrundlage benötigt wird, sondern lediglich die in Art. 6 Abs. 4 DSGVO genannten Kriterien erfüllt sein müssen. Dafür spricht der Wortlaut des Erwägungsgrunds 50 S. 2 DSGVO[168]: Wenn der ursprüngliche und der neue Zweck miteinander vereinbar sind, ist keine „andere gesonderte Rechtsgrundlage als diejenige für die Erhebung der personenbezogenen Daten [erforderlich]". Es reicht mithin aus, dass die ursprüngliche Verarbeitung, bei der es sich in aller Regel um die Erhebung der Daten handelt, auf einer Rechtsgrundlage beruht. Für die Weiterverarbeitung bei kompatiblen Zwecken muss nicht zusätzlich eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen. Das Gegenargument, Erwägungsgrund 50 DSGVO spreche nur von der „Erhebung" der Daten und beziehe sich somit nur darauf, dass die Daten nicht neu erhoben werden

---

[164] *Blum*, People Analytics, 2021, S. 233; Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 19.

[165] Vgl. BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 108; *Wehkamp*, DSRITB 2020, 215, 223.

[166] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 108.

[167] Braegelmann/Kaulartz/*Valkanova*, Kap. 8.2 Rn. 6; Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 142; EuArbRK/*Franzen*, Art. 6 DSGVO Rn. 14 f.; *Franzen*, EuZA 2017, 313, 327; *Kühling/Martini*, EuZW, 448, 454; *Wehkamp*, DSRITB 2020, 215, 223.

[168] Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 142; *Monreal*, ZD 2016, 507, 510.

müssten[169], überzeugt nicht: Die erstmalige Verarbeitung, für die es einer Rechtsgrundlage bedarf, wird immer eine „Erhebung" der Daten sein.[170] Die DSGVO differenziert nicht zwischen „Erhebung" und „Verarbeitung", sondern fasst den Verarbeitungsbegriff sehr weit: Wenn Daten *erhoben* werden, werden sie gem. Art. 4 Nr. 2 DSGVO *verarbeitet*. Erwägungsgrund 50 S. 2 DSGVO muss somit so verstanden werden, dass es für die Weiterverarbeitung keiner anderen Rechtsgrundlage als der für die ursprüngliche Verarbeitung, d. h. die Erhebung der Daten, bedarf.

Hinzu kommt, dass Art. 6 Abs. 4 DSGVO keinen Anwendungsbereich hätte, würde man neben der Kompatibilitätsprüfung noch eine zusätzliche Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO fordern. Wenn die neue Datenverarbeitung zu einem anderen Zweck auf eine Rechtsgrundlage gestützt werden kann, ist sie ohnehin rechtmäßig. Einer Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO bedarf es in dem Fall nicht mehr.

Im Ergebnis benötigt man deshalb nur für die ursprüngliche Verarbeitung eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Für die Weiterverarbeitung muss lediglich der in Art. 6 Abs. 4 DSGVO aufgeführte Kompatibilitätstest erfüllt sein. Durch die Kompatibilitätsprüfung wird sichergestellt, dass der neue und der ursprüngliche Zweck miteinander vereinbar sind.[171].

2. Einwilligung

Sind ursprünglicher und neuer Zweck nicht kompatibel, sieht Art. 6 Abs. 4 DSGVO vor, dass eine Weiterverarbeitung aufgrund einer Einwilligung möglich ist. Willigt die betroffene Person ein, disponiert sie frei über ihre personenbezogenen Daten. Allerdings ist aufgrund des

---

[169] *Blum*, People Analytics, 2021, S. 232; BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 108; S. *Schantz*, NJW 2016, 1841, 1844, der es als redaktionellen Fehler wertet, dass Erwägungsgrund 50 S. 2 so erhalten geblieben ist.

[170] BeckOK Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 35; Gola/Heckmann/*Gola*, Art. 4 DSGVO Rn. 35.

[171] Vgl. EuArbRK/*Franzen*, Art. 6 DSGVO Rn. 15, der die Anforderungen von Art. 6 Abs. 4 DSGVO verglichen mit den in Art. 6 Abs. 1 DSGVO genannten Anforderungen als enger ansieht.

Zweckbindungsgrundsatzes nach Art. 5 Abs. 1 lit. a DSGVO eine Einwilligung nur möglich, wenn die Zwecke, zu denen sie erteilt wurde, vorher explizit genannt wurden.[172] Die Zwecke dürfen nicht zu pauschal formuliert sein, wie z. B. „geschäftsmäßige Verarbeitung" oder „Marketing-Zwecke".[173] Vielmehr muss die betroffene Person erkennen, für welchen Zweck genau ihre personenbezogenen Daten verarbeitet werden. Werden Daten für Marketing-Zwecke verarbeitet, muss daher spezifiziert werden, ob damit die Werbung für Produkte der Vertragspartnerin gemeint ist oder ob die Kundendaten etwa im Unternehmensverbund weitergegeben werden.[174]

Möchte man die Daten zu Trainingszwecken bei einem maschinell lernenden System für Beförderungszwecke oder Bewerbungsprozesse nutzen, muss die Verantwortliche also den Zweck so beschreiben, dass für die betroffene Person erkennbar ist, wofür genau ihre Daten verarbeitet werden. Der (neue) auf das Training eines maschinell lernenden Systems bezogene Verarbeitungszweck muss schon bei der ursprünglichen Einwilligung erwähnt worden sein, damit die Einwilligung als Rechtsgrundlage für die Weiterverarbeitung zum neuen Zweck dienen kann. Der Zweck wäre insofern nicht mehr „neu", weil er aufgrund des Zweckbindungsgrundsatzes schon bei der ursprünglichen Einwilligung hätte erwähnt werden müssen. Ist das nicht geschehen, muss eine neue Einwilligung eingeholt werden.

Dass die Einwilligung in Art. 6 Abs. 4 DSGVO ausdrücklich genannt wurde, führt deshalb zwingend dazu, dass bei einer auf eine Einwilligung gestützten Datenverarbeitung niemals eine Weiterverarbeitung aufgrund von Zweckvereinbarkeit in Betracht kommt: Jeder Verarbeitungszweck muss in einer Einwilligung enthalten sein. In der Praxis ist somit eine *weitere* Einwilligung erforderlich, wenn man personenbezogenen Daten zu anderen Zwecken weiterverarbeiten möchte.

---

[172] Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 14; *Culik/Döpke*, ZD 2017, 226, 228.

[173] Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 14; *Klar*, BB 2019, 2243, 2246; a. A. *Niemann/Kevekordes*, CR 2020, 17, 21.

[174] Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 14.

3. Art. 54 Abs. 1 KI-VO-KOM

Bei inkompatiblen Zwecken ist es neben einer Einwilligung möglich, die Daten weiterzuverarbeiten, wenn eine Rechtsvorschrift der Union oder der Mitgliedstaaten vorliegt, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele ist. Eine solche Rechtsvorschrift ist Art. 54 Abs. 1 KI-VO-KOM.[175] Demnach dürfen im KI-Reallabor personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme unter bestimmten Bedingungen verarbeitet werden. Auf Art. 54 Abs. 1 KI-VO-KOM wird im Teil zur KI-VO-KOM näher eingegangen.[176]

4. Voraussetzungen des Kompatibilitätstests in Art. 6 Abs. 4 DSGVO

Ob der neue und der frühere Zweck miteinander vereinbar sind, richtet sich nach den Kriterien in Art. 6 Abs. 4 lit. a-e DSGVO. Die Auflistung der Kriterien ist nach dem Wortlaut des Art. 6 Abs. 4 DSGVO („unter anderem") nicht abschließend.[177] In Art. 6 Abs. 4 DSGVO sind folgende Kriterien genannt:

- die Verbindung zwischen dem ursprünglichen und dem neuen Zweck (Art. 6 Abs. 4 lit. a DSGVO);
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere im Hinblick auf das Verhältnis zwischen betroffener Person und Verantwortlicher (Art. 6 Abs. 4 lit. b DSGVO);
- die Art der personenbezogenen Daten (Art. 6 Abs. 4 lit. c DSGVO);
- die Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (Art. 6 Abs. 4 lit. d DSGVO) und
- das Vorhandensein geeigneter Garantien, z. B. die Verschlüsselung oder Pseudonymisierung (Art. 6 Abs. 4 lit. e DSGVO).

Anhand dieser Kriterien wird geprüft, ob die Zwecke miteinander kompatibel sind. Darin liegt eine Abwägung, bei der alle Umstände der Verarbeitung

---

[175] S. dazu Kapitel 11 E. (S. 384).
[176] Kapitel 11 E. (S. 384).
[177] Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 48.

berücksichtigt werden. Um den Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO durchzuführen, müssen alle denkbaren Kriterien, die bei der Datenverarbeitung eine Rolle spielen, berücksichtigt werden.[178]

Eine Ausnahme gilt, wenn die Daten aufgrund im öffentlichen Interesse liegender Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken weiterverarbeitet werden. Dann wird gem. Art. 5 Abs. 1 lit. b i. V. m. Art. 89 DSGVO vermutet, dass der neue Zweck mit dem ursprünglichen kompatibel ist. Werden personenbezogene Daten zu Trainingszwecken maschinell lernender Systeme verwendet, die im Bewerbungsverfahren oder bestehenden Arbeitsverhältnis eingesetzt werden sollen, werden die Daten nicht zu Archivzwecken, wissenschaftlichen, historischen oder statistischen Zwecken verarbeitet. Die Ausnahme ist für den Untersuchungsgegenstand der Arbeit nicht relevant.

a) Maßstab

Für die Auslegung können die durch die Art. 29-Datenschutzgruppe[179] vorgegebenen Anhaltspunkte herangezogen werden, die im Folgenden dargelegt werden.[180] In der DSRL war die Zweckänderung nicht detailliert geregelt, sondern wurde allein in Art. 6 Abs. 1 lit. b DSRL erwähnt. Kriterien wie in Art. 6 Abs. 4 lit. a-f DSGVO enthielt Art. 6 Abs. 1 lit. b DSRL nicht. Die Kriterien, auf die die Art. 29-Datenschutzgruppe eingeht, wurden von den Mitgliedstaaten entwickelt.[181] Sie stimmen mit den Kriterien, die später in Art. 6 Abs. 4 DSGVO aufgenommen wurden, überein, sodass Aussagen der Art. 29-Datenschutzgruppe für die Auslegung der Merkmale nach Art. 6 Abs. 4 lit. a-f DSGVO berücksichtigt werden können.[182]

Art. 6 Abs. 4 lit. a DSGVO fordert zunächst, dass bei der Frage, ob ursprünglicher und neuer Zweck kompatibel sind, die Verbindung zwischen den Zwecken berücksichtigt werden soll. Nach Ansicht der Art. 29-

---

[178] Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 135.

[179] Zur Art. 29-Datenschutzgruppe s. Kapitel 5 A.III.1.a) (S. 63).

[180] *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation (WP 203), S. 23 ff.

[181] *Dies.*, Opinion 03/2013 on purpose limitation (WP 203), S. 23.

[182] Braegelmann/Kaulartz/*Valkanova*, S. 338 Rn. 7.

Datenschutzgruppe liegt eine Verbindung des ursprünglichen und des neuen Zwecks vor, wenn der neue Zweck logische oder naheliegende Folge der ursprünglichen Zweckbestimmung ist. Je größer der Unterschied zwischen dem ursprünglichen Verarbeitungszweck und dem neuen Zweck der Weiterverarbeitung sei, desto problematischer sei die Vereinbarkeit der beiden Zwecke miteinander.

Berücksichtigt wird außerdem der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden (Art. 6 Abs. 1 S. 1 lit. b DSGVO): Zu prüfen ist nach Ansicht der Art. 29-Datenschutzgruppe, was eine verständige Person anstelle der betroffenen Person erwarten wird, was basierend auf der Datenverarbeitung mit ihren Daten geschieht. Je überraschender die Weiterverarbeitung zu einem anderen Zweck sei, desto eher sei der neue Zweck inkompatibel mit dem ursprünglichen Zweck.

Gem. Art. 6 Abs. 4 lit. c DSGVO wird berücksichtigt, ob besondere Kategorien personenbezogener Daten verarbeitet werden. Je mehr sensible Daten verarbeitet werden würden, desto eher seien die Zwecke nicht miteinander vereinbar und eine Weiterverarbeitung zu einem anderen Zweck ausgeschlossen.

Bei den möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (Art. 6 Abs. 4 lit. d DSGVO) seien sowohl negative als auch positive Konsequenzen zu berücksichtigen. Das könnten potenzielle zukünftige Entscheidungen sein oder Handlungen von Dritten und Situationen, in denen die Weiterverarbeitung zur Ausgrenzung oder Benachteiligung von Personen führe. Hinzu komme die Art, wie die Daten weiterverarbeitet würden, z. B. wenn eine neue Verantwortliche die Daten weiterverarbeite.

Geeignete Garantien für die Daten (Art. 6 Abs. 4 lit. e DSGVO) seien u. a. die vollständige Anonymisierung, die Teilanonymisierung und die Pseudonymisierung.

Wie die Kriterien gewichtet werden, d. h., ob z. B. eine Zweckänderung eher zulässig ist, wenn ein bestimmtes Kriterium des Art. 6 Abs. 4 DSGVO

vorliegt, gibt die Norm nicht vor. Die Stellungnahme der Art. 29-Datenschutzgruppe legt aber nahe, dass geeignete Garantien als Kompensation für die Zweckänderung dienen können. [183] Ob die Verarbeitung zu einem neuen Zweck zulässig ist, hängt aber von der gesamten Prüfung der Kriterien ab.[184] Die Verantwortliche muss abwägen, begründen und dokumentieren, warum in dem konkreten Fall eine Zweckänderung zulässig sei.[185]

b) Verbindung der Zwecke beim Training maschinell lernender Systeme

Anbieterinnen maschinell lernender Systeme können die Daten ihrer Auftraggeberinnen nutzen, um ihr System weiter zu verbessern. Dass bereits gesammelte Daten für Trainingszwecke eines maschinell lernenden Systems genutzt werden, ist nicht unbedingt die logische oder naheliegende Folge der ursprünglichen Zweckbestimmung. Auch würde eine verständige Person an Stelle der betroffenen Person nicht davon ausgehen, dass die personenbezogenen Daten zu Zwecken des Trainings eines maschinell lernenden Systems weiterverarbeitet werden. Hat sich eine Arbeitnehmerin in einem Unternehmen beworben, wird sie nicht davon ausgehen, dass ihre Daten für Trainingszwecke eines maschinell lernenden Systems genutzt werden. Die Weiterverarbeitung wird auch nicht für die konkreten Arbeitnehmerinnen vorteilhaft sein, sondern – wenn überhaupt – nur für zukünftige Bewerberinnen. Wird aber ein maschinell lernendes System mit den Daten trainiert, um interne Beförderungsprogramme zu verbessern, kann darin ein Mehrwert für die betroffenen Personen liegen. Die Weiterverarbeitung der Daten kann nach den Umständen des Einzelfalls dazu führen, dass die bestehende Vertragsbeziehung verbessert wird. Darin kann man einen rechtlichen und tatsächlichen Zusammenhang sehen, was für eine Verbindung der Zwecke nach Art. 6 Abs. 4 DSGVO spricht.[186]

---

[183] *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation (WP 203), S. 26.
[184] *Dies.*, Opinion 03/2013 on purpose limitation (WP 203), S. 26.
[185] Vgl. Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 175.
[186] Vgl. Braegelmann/Kaulartz/*Skistims*, S. 375 Rn. 60.

c) Art der personenbezogenen Daten

Werden personenbezogene Daten von Bewerberinnen oder Arbeitnehmerinnen zu einem anderen Zweck weiterverarbeitet, muss die Art der personenbezogenen Daten berücksichtigt werden, d. h. insbesondere, ob etwa sensible Daten gem. Art. 9 DSGVO verarbeitet werden. Diese Daten sind besonders schutzbedürftig. Je sensibler die Daten sind, desto eher scheidet eine Zweckvereinbarkeit aus. [187] Werden personenbezogene Daten von Bewerberinnen oder Arbeitnehmerinnen weiterverarbeitet, kann es sich dabei um sensible Daten nach Art. 9 Abs. 1 DSGVO handeln. Wird z. B. ein Portraitfoto verarbeitet, das eine Brillenträgerin zeigt, lässt das Rückschlüsse auf eine medizinische Information – die Stärke ihrer Sehkraft – zu. Es handelt sich daher um ein Gesundheitsdatum.[188]

d) Folgen der Weiterverarbeitung für die betroffene Person

Außerdem müssen die Folgen der Weiterverarbeitung für die betroffene Person berücksichtigt werden. Dienen die Daten als Trainingsdaten für ein bestimmtes maschinell lernendes System, mit dem die betroffene Person auch nicht weiter in Berührung kommt, kann man davon ausgehen, dass es sich nicht auf die betroffene Person auswirkt, wenn ihre Daten weiterverarbeitet werden. Allerdings ist es je nach den ergriffenen Schutzmaßnahmen für die personenbezogenen Daten abhängig, ob nicht ggf. nach Abschluss des Trainings auf die personenbezogenen Daten zurückgegriffen werden kann.[189] Die Folgen der Weiterverarbeitung müssen aber unmittelbar bevorstehen. Hypothetische Folgen sollen nicht in die Abwägung einbezogen werden, ohne dass es dafür Anhaltspunkte gibt. Ansonsten müsste man auch berücksichtigten, dass das trainierte System in späterer Zukunft bei einer Bewerbung der betroffenen Person eingesetzt wird, deren Daten bereits im Trainingsprozess verarbeitet wurden. Ob das maschinell lernende System nur ausschließlich negative oder positive Folgen für die betroffene Person hat, ist nicht immer von vornherein zu sagen. Wird das maschinell lernende System für die Frage einer zusätzlichen Leistungsgewährung aufgrund von besonders

---

[187] *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation (WP 203), S. 25; *Blum*, People Analytics, 2021, S. 243; *Meinecke*, Datenschutz und Data Science, 2021, S. 217.

[188] Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 109.

[189] Dazu sogleich: Kapitel 6 B.IV.4.e) (S. 142).

guter Arbeit eingesetzt, kann es positiv sein, wenn das maschinell lernende System die betroffene Person für die Leistungsgewährung vorschlägt. Umgekehrt kann es aber auch nachteilig sein, wenn man eine Zusatzvergütung aufgrund der Vorauswahl des maschinell lernenden Systems nicht erhält. Negativ ist jedenfalls das Szenario zu bewerten, wenn die zweckändernde Verarbeitung etwa dazu führt, dass Kündigungen ausgesprochen werden.[190]

Die Verantwortliche muss im Vorhinein analysieren, abwägen und begründen, welche Folgen die Weiterverarbeitung der personenbezogenen Daten für die betroffene Person hat. Je mehr negative Auswirkungen die Weiterverarbeitung auf die betroffene Person haben könnte, desto eher ist es unzulässig, die Daten zu einem neuen Zweck weiterzuverarbeiten.

e) Vorhandensein geeigneter Garantien

In dem Fall, dass personenbezogene Daten als Trainingsdaten genutzt werden, müssen auch die vorhandenen Garantien zum Schutz personenbezogener Daten berücksichtigt werden (Art. 6 Abs. 4 lit. d DSGVO). Je stärker der Personenbezug verringert werden kann, umso eher ist es möglich, die Daten weiterzuverarbeiten.[191]

Hervorzuheben ist an dieser Stelle, dass es beim Training eines maschinell lernenden Systems nicht auf den konkreten Personenbezug ankommt, sondern nur darauf, dass Informationen über irgendwelche Personen vorliegen.[192] Das auf Basis der einzelnen Daten trainierte System setzt sich zwar aus den einzelnen Werten der Daten zusammen. Am Ende ist das maschinell lernende System, welches auf neue Daten angewendet wird, aber nicht mehr personenbezogen.[193] Die Algorithmen, aus denen sich das „fertig trainierte" System zusammensetzt, lassen für sich genommen keine unmittelbaren Rückschlüsse auf die (personenbezogenen) Trainingsdaten zu.[194] Man ging daher zunächst davon aus, dass es unmöglich ist, auf die Trainingsdaten

---

[190] *Götz*, Big Data im Personalmanagement, 2020, S. 132.
[191] Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 50.
[192] *Niemann/Kevekordes*, CR 2020, 17, 21.
[193] *Marx/Sütthoff*, ZdiW 2022, 128, 130.
[194] *Dies.*, ZdiW 2022, 128, 130.

zurückzugreifen.[195] Das Training führte nach dieser Annahme somit zu einer Anonymisierung der Trainingsdaten.[196] Allerdings ist es mithilfe gezielter Attacken gegen trainierte Modelle möglich, Rückschlüsse auf die ursprünglichen Daten herzustellen.[197]

Mithilfe der sog. *membership-inference-attacks* ist es nachweisbar, dass bestimmte Trainingsdaten zum Trainieren verwendet worden sind. Wenn das maschinell lernende System auf der Grundlage eines bestimmten Trainingsdatums ein Ergebnis mit einer Übereinstimmung von 100% generiert, liegt es nahe, dass dieses Datum Teil der Trainingsdaten war. Man benötigt also entsprechende *Input-Daten*, um *membership-inference-attacks* durchzuführen.

Bei sog. *model-inversion-attacks* lassen sich Trainingsdaten rekonstruieren, wenn man vereinzelte Daten kennt.[198] Beispielsweise war es bei einem Modell, das anhand genetischer Biomarker die richtige Dosierung eines Medikaments ermitteln sollte, möglich, anhand einiger demografischer Informationen über bestimmte Patientinnen deren genetische Biomarker aufzudecken.[199]

Auch wenn es vor diesem Hintergrund möglich ist, Rückschlüsse auf Trainingsdaten auch nach dem Training eines Modells zu erhalten, wird das praktische Risiko eher gering sein. Bei beiden Angriffsszenarien benötigt man gewisse Kenntnisse der Modelle und Kenntnisse über bestimmte Daten.[200] Um derartige Attacken aber zu vermeiden, kann man bestimmte Schutzmechanismen vorsehen.[201] Etwa ist es möglich, den Daten statistische

---

[195] *Boenisch*, DuD 2021, 448; *Maltzan/Käde*, DSRITB 2020, 505, 506.

[196] *Boenisch*, DuD 2021, 448.

[197] *Battis/Graner*, in: Reussner/Koziolek/Heinrich (Hrsg.), Informatik 2020, Lecture Notes in Informatics (LNI), 2021, 841-853, 842 f.; *Boenisch*, DuD 2021, 448; *Veale/Binns/Edwards*, Philosophical Transactions 2018, 1, 5 f.

[198] Braegelmann/Kaulartz/*Kaulartz*, S. 466 Rn. 12; *Battis/Graner*, in: Reussner/Koziolek/Heinrich (Hrsg.), Informatik 2020, Lecture Notes in Informatics (LNI), 2021, 841-853, 843 f.; *Boenisch*, DuD 2021, 448, 450.

[199] *Veale/Binns/Edwards*, Philosophical Transactions 2018, 1, 6.

[200] Braegelmann/Kaulartz/*Kaulartz*, S. 466 Rn. 13.

[201] *Battis/Graner*, in: Reussner/Koziolek/Heinrich (Hrsg.), Informatik 2020, Lecture Notes in Informatics (LNI), 2021, 841-853, 850 f.

Störungen und Rauschen hinzufügen (sog. *differential privacy*)[202], sodass das Risiko der Identifizierung einer natürlichen Person verringert wird.[203] Wenn geeignete Maßnahmen ergriffen worden sind, um die personenbezogenen Daten einzelner Individuen auch vor etwaigen Attacken zu schützen, spricht das eher für eine mögliche Weiterverarbeitung. Wenn es möglich ist, muss die Verantwortliche die Daten zur Weiterverarbeitung anonymisieren.[204] Eine wirksame Anonymisierung im rechtlichen Sinn liegt aber nur vor, wenn der Personenbezug der Daten aufgehoben wurde.[205] Ist dies nicht möglich, muss die Verantwortliche die Daten pseudonymisieren.[206] Im Einzelfall sind mithin die technischen Lösungen anzupassen. In jedem Fall muss die Verantwortliche die Maßnahmen dokumentieren, damit sie etwa nachweisen kann, dass sie die Datenschutzgrundsätze wie etwa den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO eingehalten hat.

f) Zwischenergebnis: hohe Anforderungen des Kompatibilitätstests

1. Ob die Weiterverarbeitung zu einem anderen Zweck mit dem ursprünglichen Zweck vereinbar ist, muss anhand einer umfassenden Einzelfallabwägung unter Berücksichtigung der in Art. 6 Abs. 4 lit a-f DSGVO aufgeführten Kriterien getroffen werden.[207] Die Anforderungen des sog. Kompatibilitätstest sind hoch.

2. Für die betroffene Person ist es nicht naheliegend, dass ihre personenbezogenen Daten zu Trainingszwecken eines maschinell lernenden Systems, das im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis eingesetzt werden soll, weiterverarbeitet werden. Es liegt somit nicht nahe, dass die beiden Zwecke miteinander verbunden sind i. S. d. Art. 6 Abs. 4 lit. a DSGVO.[208] Die möglichen Folgen der

---

[202] S. dazu schon bereits unter: Kapitel 6 B.I.2.

[203] Braegelmann/Kaulartz/*Kaulartz*, S. 467 Rn. 14; *Battis/Graner*, in: Reussner/Koziolek/Heinrich (Hrsg.), Informatik 2020, Lecture Notes in Informatics (LNI), 2021, 841-853, 851 f.; *Boenisch*, DuD 2021, 448, 460.

[204] S. dazu bereits unter: Kapitel 6 B.I.

[205] Kapitel 6 B.II. (S. 121).

[206] Kapitel 6 B.VI.2.a) (S. 155).

[207] Kapitel 6 B.IV.4. (S. 137).

[208] Kapitel 6 B.IV.4.b) (S. 140).

Weiterverarbeitung hängen maßgeblich davon ab, wie hoch die geeigneten Garantien für die betroffene Person sind.[209] Werden die Daten zu Trainingszwecken des maschinell lernenden Systems weiterverarbeitet, sind die Folgen der Weiterverarbeitung für die betroffene Person gering, wenn ihre Daten hinreichend geschützt sind.

3. Wenn geeignete Maßnahmen ergriffen worden sind, um die personenbezogenen Daten einzelner Individuen auch vor etwaigen Attacken (z. B. *membership-inference-attacks*) zu schützen, spricht das eher für eine mögliche Weiterverarbeitung. Wenn es möglich ist, muss die Verantwortliche die Daten zur Weiterverarbeitung anonymisieren.[210]

V. Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO

Neben der Möglichkeit der Zweckänderung nach Art. 6 Abs. 4 DSGVO kann die Verantwortliche auch neue personenbezogene Daten verarbeiten. Als Rechtsgrundlage kommt dafür eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO in Betracht. Gem. Art. 4 Nr. 11 DSGVO versteht die DSGVO eine Einwilligung als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist". Willigt die betroffene Person der Verarbeitung der sie betreffenden personenbezogenen Daten für einen bestimmten oder mehrere bestimmte Zwecke ein, ist die Verarbeitung der Daten gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO rechtmäßig. Die Einwilligung drückt die informationelle Selbstbestimmung aus, denn sie versetzt die betroffene Person in die Lage, über das „Ob" und „Wie" der Verarbeitung ihrer personenbezogenen Daten zu bestimmen.[211] Die Voraussetzungen für eine wirksame Einwilligung ergeben sich aus einer

---

[209] Kapitel 6 B.IV.4.e) (S. 142).

[210] S. dazu bereits unter: Kapitel 6 B.I. (S. 118).

[211] Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 17; kritisch zum Institut der Einwilligung s. etwa *Hoffmann-Riem*, AöR 142 (2017), 1, 21 f.

Zusammenschau von Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, 7 DSGVO i. V. mit deren Erwägungsgründen.[212]

1. Formelle Voraussetzungen

Die Einwilligung kann in jeder beliebigen Form erteilt werden. Wird die Einwilligung durch eine schriftliche Erklärung erteilt, die noch andere Sachverhalte betrifft, muss das Ersuchen um die Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Die Frage nach der Einwilligung muss sich eindeutig von den anderen Sachverhalten unterscheiden (Art. 7 Abs. 2 S. 1 DSGVO).

2. Materielle Voraussetzungen

a) Freiwilligkeit als zentrales Kriterium

Zentrales Kriterium der Einwilligung ist, dass sie freiwillig erteilt werden muss.[213] Freiwillig erteilt wird die Einwilligung dann, wenn die betroffene Person eine echte oder freie Wahl hat und in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen.[214] Beim Merkmal der „Freiwilligkeit" muss gem. Art. 7 Abs. 4 DSGVO auch dem Umstand Rechnung getragen werden, ob von der Einwilligung etwa die Erfüllung eines Vertrags abhängig ist.[215]

Im Arbeitsverhältnis besteht ein besonderes Abhängigkeitsverhältnis [216] zwischen Arbeitgeberin und Arbeitnehmerin, weshalb an das Merkmal der Freiwilligkeit der Einwilligung besonders hohe Anforderungen gestellt werden.[217] Wird die Einwilligung eingeholt, um personenbezogene Daten zu Trainingszwecken zu verarbeiten, liegt aber meist kein konkretes

---

[212] Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 18.

[213] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 34; *Hofmann*, DSRITB, 209, 213.

[214] Erwägungsgrund 42 S. 5 DSGVO; Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 7; Jandt/Steidle/*Wilmer*, B II. 2. Rn. 89.

[215] Dazu sogleich: Kapitel 6 B.V.2.b) (S. 147).

[216] *BT-Drs. 18/11325*, S. 30; Taeger/Gabel/*Taeger*, Art. 7 DSGVO Rn. 105; *Däubler*, Gläserne Belegschaften, 9. Aufl. 2021, § 4 Rn. 152 f.; *Herfurth*, ZD 2018, 514, 518.

[217] *Ernst*, ZD 2017, 110, 112 *Folkerts*, DuD 2022, 77; *Schmidt/Plote*, NZA 2022, 1297, 1300; s. dazu genauer auch unter: Kapitel 6 C.III.1. (S. 163).

Beschäftigungsverhältnis vor, weshalb auch nicht die (zusätzlichen) Anforderungen des § 26 Abs. 2 BDSG zu berücksichtigen sind.[218]

b) Rechnungstragungsgebot gem. Art. 7 Abs. 4 DSGVO

In Bezug auf Art. 7 Abs. 4 DSGVO ist häufig von einem „Kopplungsverbot"[219] die Rede: Die Erfüllung eines Vertrags dürfe nicht von der Einwilligung in die Verarbeitung personenbezogener Daten abhängig sein, welche nicht zur Abwicklung des Geschäfts erforderlich sind. [220] Das Kopplungsverbot schütze die freie und eigenständige Willensbetätigung der Nutzerin bei der Einwilligung und verhindere, dass ein faktischer Zwang zur Einwilligung bei einer bestimmten Datenverwendung entstehe.[221]

Das Kopplungsverbot in Art. 6 Abs. 4 DSGVO sei jedoch nicht als ein absolutes Kopplungsverbot zu verstehen:[222] Eine Einwilligung sei nicht immer unfreiwillig, weil sie an einen Vertragsschluss gekoppelt sei.

Gemäß dem Wortlaut des Art. 7 Abs. 4 DSGVO muss „bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, [..] dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind". Es wird nicht jede „Kopplung" einer Einwilligung an eine Vertragserfüllung verboten, vielmehr soll „dem Umstand Rechnung getragen werden", ob die Einwilligung an eine Vertragserfüllung geknüpft ist. Daraus ergibt sich, dass bei der Beurteilung der Freiwilligkeit abgewogen werden muss, ob die Einwilligung in eine Datenverarbeitung über das für eine Vertragserfüllung erforderliche Maß hinausgeht.[223] Statt von einem Kopplungsverbots sollte

---

[218] S. dazu unter: Kapitel 6 C.III. (S. 163).

[219] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 34; Ehmann/Selmayr/*Heckmann/Paschke*, Art. 7 DSGVO Rn. 94; Sydow/Marsch/*Ingold*, Art. 7 DSGVO Rn. 30; Spindler/Schuster/*Spindler/Dalby*, Art. 7 DSGVO Rn. 14.

[220] Ehmann/Selmayr/*Heckmann/Paschke*, Art. 7 DSGVO Rn. 94.

[221] Ehmann/Selmayr/*dies.*, Art. 7 DSGVO Rn. 94.

[222] Ehmann/Selmayr/*dies.*, Art. 7 DSGVO Rn. 95.

[223] Kühling/Buchner/*Buchner/Kühling*, Art. 7 DSGVO Rn. 46.

man daher eher von einem Rechnungstragungsgebot oder einer Prüfpflicht sprechen.[224] Zwar trifft Erwägungsgrund 43 S. 2 DSGVO folgende Aussage: Eine Einwilligung gilt nicht als freiwillig erteilt, wenn die Erfüllung eines Vertrags von ihr abhängig ist. Die Formulierung „abhängig ist" könnte man als Kopplungsverbot verstehen. Der Wortlaut von Erwägungsgründe ist jedoch nicht so verbindlich wie der Wortlaut einer Vorschrift.[225] Vielmehr ist davon auszugehen, dass der Gesetzgeber zwischen Erwägungsgründen und den konkreten Vorschriften differenziert und man sich insbesondere hinsichtlich des Zwecks einer Vorschrift auf Erwägungsgründe beziehen kann. Hätte der Verordnungsgeber ein absolutes Verbot bezweckt, hätte er ein solches explizit in den Verordnungstext aufnehmen können. Ausgangspunkt ist somit immer der Wortlaut der Norm, der nur im Lichte des Erwägungsgrundes auszulegen ist.[226]

Im Einzelfall müssen somit die Bedeutung der Leistung und diejenigen der bezweckten Datenverarbeitung ins Verhältnis zueinander gesetzt werden.[227] Zulässig ist es, die Art der Leistungserbringung von der Einwilligung in die Datenverarbeitung abhängig zu machen, wenn die Datenverarbeitung „notwendige Entscheidungs- und Kalkulationsgrundlage für das konkrete Rechtsgeschäft" ist.[228] Beim Abschluss einer Versicherung kann die Versicherin das „Ob" und „Wie" der Versicherung davon abhängig machen, welche Daten der Versicherungsinteressent preisgibt.[229] Schließlich ergibt sich aus bestimmten Daten, wie zuverlässig etwa die Interessentin ist.

Werden Trainingsdaten gesammelt, kann es sein, dass die Einwilligung unabhängig oder abhängig davon erteilt wird, ob ein Vertrag erfüllt wird. Zwar geht es nicht zwingend um die Begründung eines konkreten Beschäftigungsverhältnisses, wenn Trainingsdaten gesammelt werden. Die

---

[224] *Engeler*, ZD 2018, 55, 59.

[225] Kapitel 5 A.III.1. (S. 62).

[226] Kapitel 5 A.III.1. (S. 62).

[227] *Engeler*, ZD 2018, 55, 59.

[228] *Kühling/Buchner*, in: Datenschutz-Grundverordnung BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 47.

[229] *Kühling/Buchner*, in: Datenschutz-Grundverordnung BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 47.

Arbeitgeberin kann die Datenverarbeitung aber auch als Voraussetzung für die Begründung eines Vertragsverhältnisses einsetzen, z. B. wenn eine Bewerberin in die Datenverarbeitung zu Trainingszwecken einwilligen muss, um am Bewerbungsprozess teilzunehmen. [230] In einem solchen Fall ist die Einwilligung abhängig von einem Vertragsschluss und kann mithin nicht freiwillig erteilt werden. Holt die verantwortliche Person die Einwilligung zu Trainingszwecken gesondert ein und kann die betroffene Person, ohne Nachteile zu erleiden, ggf. ablehnen, dass ihre Daten zu Trainingszwecken verarbeitet werden, liegt Freiwilligkeit vor.[231] Die Verantwortliche sollte den Vorgang dokumentieren, damit sie nachweisen kann, dass die Einwilligung freiwillig erteilt worden ist und nicht von einem Vertragsschluss abhängig gemacht worden ist.

c) Bestimmtheit

Die Einwilligung muss zudem für einen bestimmten Zweck oder mehrere bestimmte Zwecke erteilt werden. Eine pauschale Einwilligung, die sich auch auf unklare Zwecke erstreckt, ist nicht zulässig.[232] Ist etwa noch nicht klar, zu welchen Trainingszwecken personenbezogene Daten verarbeitet werden sollen, kann eine Einwilligung mangels Bestimmtheit nicht erteilt werden. Wird in die Datenverarbeitung eingewilligt, muss für die betroffene Person deutlich sein, für welches maschinell lernende System genau ihre Daten als Trainingsdaten verwendet werden. So reicht es nicht aus, dass der betroffenen Person mitgeteilt wird, es handele sich um das Training eines maschinell lernenden Systems zur Bewerberinnenvorauswahl. Der betroffenen Person muss das konkrete System sowie der Einsatzbereich des Systems vorgestellt werden. Außerdem muss die betroffene Person auch darüber informiert werden, auf welche Merkmale hin ihre Daten analysiert werden und welche Schutzmaßnahmen für ihre Daten ergriffen werden[233].

---

[230] Kapitel 6 B.IV.2. (S. 135).

[231] Vgl. *Kuß*, in: Kuß/Steege/Chibanguza (Hrsg.), Künstliche Intelligenz, 2022, G. Beschäftigtendatenschutz Rn. 18.

[232] Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 9; *Wehkamp*, DSRITB 2020, 215, 222; noch zur DSRL s. *Härting*, NJW 2015, 3284, 3286 ff.

[233] Dazu sogleich: Kapitel 6 B.V.2.d) (S. 150).

d) Informiertheit der Einwilligung

Die Einwilligung muss „in informierter Weise" abgegeben werden (Art. 4 Nr. 11 DSGVO). Die betroffene Person muss abschätzen können, welche Folgen ihre Einwilligung hat. Sie muss die Umstände der Datenverarbeitung sowie die Tragweite ihrer Einwilligung eindeutig erkennen können.[234]

Werden algorithmische Systeme eingesetzt, sollte die betroffene Person nicht nur darüber informiert werden, welche Daten zu welchen Zwecken verarbeitet werden, sondern auch darüber, welche Risiken möglicherweise für sie mit dem Einsatz des algorithmischen Systems einhergehen. Nur, wenn die Person diese Informationen erhält, kann sie die Einwilligung „in Kenntnis der Sachlage" abgeben. Die Vorgänge müssen für die betroffene Person mithin *transparent* sein. Beim Einsatz von maschinell lernenden Systemen ist die Informiertheit eine Herausforderung: Die Transparenz eines solchen Systems durch Erklärbarkeit und Nachvollziehbarkeit zustande.[235] Die beiden Aspekte werden – wie bereits ausgeführt worden ist[236] – im Kontext dieser Arbeit wie folgt verstanden: Erklärbarkeit meint, dass die betroffene Person verstehen muss, welche Komponenten für die konkrete Entscheidung relevant waren. Nachvollziehbar ist die Entscheidung dann, wenn die Person die grundsätzliche Funktionsweise des maschinell lernenden Systems versteht, um Risiken und Chancen einordnen zu können. Es ist nicht erforderlich, dass die Person umfassend versteht, wie das maschinell lernende System funktioniert.

Übertragen auf die Informiertheit der Einwilligung müsste die Verantwortliche der Person aufzeigen, welche Risiken für ihre personenbezogenen Daten nach dem Training des Systems bestehen können. Das bedeutet konkret, die betroffene Person über den Schutz der personenbezogenen Daten zu informieren: Werden die Daten anonymisiert oder pseudonymisiert? Wie hoch ist die Gefahr, dass nach dem Training noch Rückschlüsse auf die personenbezogenen Daten gezogen werden können?[237]

---

[234] Kühling/Buchner/*Buchner/Kühling*, Art. 7 DSGVO Rn. 59; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 40; kritisch dazu: *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 77 ff.

[235] Kapitel 4 (S. 39).

[236] Kapitel 4 B.I. (S. 45).

[237] Vgl. Kapitel 6 B.IV.4.e) (S. 142).

Es wird aber kaum möglich sein, pauschal alle möglichen Risiken aufzuzeigen, weil man auch als Verantwortliche nicht genau weiß, welche potentiellen Gefahren für die personenbezogenen Daten nach der Verarbeitung bestehen. Insbesondere kann man nicht abschätzen, ob die getroffenen Schutzmaßnahmen ausreichen, die personenbezogenen Daten hinreichend zu sichern. Schließlich gibt es immer wieder neue technische Entwicklungen, die einen Zugriff auf Daten ermöglichen und bei denen die getroffenen Schutzmaßnahmen womöglich nicht ausreichen.

Die Transparenzanforderungen dürfen für die Verantwortlichen aber auch nicht zu hoch werden. Ausreichend sollte sein, wenn die Verantwortliche aufzeigt, welche Risikomaßnahmen sie für die Daten, die konkret verarbeitet werden, ergreift. Außerdem kann sie darlegen, ob das algorithmische System etwa nur unternehmensintern eingesetzt wird oder gar an Dritte verkauft wird.[238] Letzteres würde das Risiko für die betroffene Person weiter erhöhen.

3. Widerruf der Einwilligung

Gem. Art. 7 Abs. 3 S. 1 DSGVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Ein sachlicher Grund ist nicht erforderlich.[239] Der Widerruf wirkt für die Zukunft.[240] Die Verarbeitung der Daten bis zum Widerruf bleibt rechtmäßig, vgl. Art. 7 Abs. 3 S. 2 DSGVO. Wenn die betroffene Person ihre Einwilligung widerruft, muss die Verantwortliche die personenbezogenen Daten unverzüglich löschen, Art. 17 Abs. 1 lit. b DSGVO. Sie müssen allerdings nicht gelöscht werden, wenn eine anderweitige Rechtsgrundlage für die Verarbeitung besteht.

Bei maschinell lernenden Systemen muss die Verantwortliche also zunächst prüfen, ob eine anderweitige Rechtsgrundlage für die Verarbeitung besteht.[241]

---

[238] *Kollmar/El-Auwad*, DSRITB 2020, 199, 205.

[239] BeckOK Datenschutzrecht/*Stemmer*, Art. 7 DSGVO Rn. 92; Ehmann/Selmayr/*Heckmann/Paschke*, Art. 7 DSGVO Rn. 86; Braegelmann/Kaulartz/*Skistims*, Kapitel 8.2 Rn. 21; *Hacker*, ZfPW 2019, 148, 178; *Hitzelberger-Kijima*, öAT 2020, 133, 135; vgl. *Uecker*, ZD 2019, 248.

[240] Arnold/Günther Arb. 4.0-Hdb/*Hamann/Haußmann*, § 6 Rn. 82; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 38; *Gausling*, DSRITB 2018, 519, 531.

[241] S. dazu unter: Kapitel 6 A.III. (S. 110).

Ist das nicht der Fall, müssen die personenbezogenen Daten gelöscht werden. Trainingsdaten können grundsätzlich nur aus dem trainierten Modell gelöscht werden, wenn das ganze Modell ohne die betroffenen Daten neu trainiert wird.[242] Es ist aber auch möglich, Daten zu löschen, ohne das Modell neu zu trainieren. Technisch ist das sehr komplex und soll an dieser Stelle daher nicht weiter vertieft werden.[243]

Gausling schlägt vor, dass man zwar nicht die Trainingsdaten weiter nutzen dürfe, die weitere Entwicklung des auf den Trainingsdaten basierenden Algorithmus aber weiterhin möglich sein müsse.[244] Die KI-Entwicklung werde ansonsten unnötig behindert. Dabei lässt sie aber den Aspekt außer Acht, dass auch bei trainierten Systemen ein Rückschluss auf die personenbezogenen Daten möglich ist.[245] Wenn die Einwilligung widerrufen wird, darf die betroffene Person aber erwarten, dass für sie kein Risiko mehr besteht, weshalb der Vorschlag von *Gausling* nicht uneingeschränkt gelten kann. Vielmehr darf man das maschinell lernende System nur weiter verwenden, wenn eine Re-Identifikation ausgeschlossen ist. Wie bereits herausgearbeitet worden ist, kann in diesem Fall das Anonymisieren mit dem Löschen gleichgesetzt werden.[246] Dann liegt auch eine wirksame Anonymisierung im Rechtssinne vor. Sind die personenbezogenen Daten anonymisiert, muss es daher möglich sein, dass maschinell lernende System trotz des Widerrufs weiterzuverwenden.[247] Andernfalls müssen die Daten aus dem maschinell lernenden System gelöscht werden. Das kann im Einzelfall auch bedeuten, dass das maschinell lernende System nicht mehr verwendet werden darf, wenn die Daten nicht gelöscht werden können.

---

[242] *Antonio Ginart/Melody Guan/Gregory Valiant u.a.*, NIPS'19: Proceedings of the 33rd International Conference on Neural Information Processing Systems 2019, 3518.

[243] S. dazu etwa: *dies.*, NIPS'19: Proceedings of the 33rd International Conference on Neural Information Processing Systems 2019, 3518.

[244] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 45; a. A. *Conrad*, DSRITB 2019, 391, 402, der vor einer Aushöhlung des Betroffenenrechts warnt.

[245] Dazu bereits unter: Kapitel 6 B.IV.4.d) (S. 141).

[246] S. dazu: Kapitel 6 B.II.3.c) (S. 129).

[247] In die Richtung auch: Braegelmann/Kaulartz/*Skistims*, S. 358 Rn. 21.

4. Zwischenergebnis: Einwilligung ist keine rechtssichere Grundlage

1. Werden Daten zum Training maschinell lernender Systeme für die Bewerberinnenvorauswahl gesammelt, kann die Einwilligung freiwillig erteilt werden, wenn es nicht um ein konkretes Beschäftigungsverhältnis geht. Wird die Einwilligung zum Training des maschinell lernenden Systems im Zusammenhang mit einer konkreten Bewerbung eingeholt, muss sie gesondert erfolgen.

2. Außerdem muss sichergestellt werden, dass die Bewerbung nicht davon abhängt, ob man in die Weiterverarbeitung der Daten einwilligt. Das kann man etwa darüber sicherstellen, dass die Unternehmen, die das System anbieten und die entsprechenden Daten an die Arbeitgeberin übermitteln, die Information darüber, ob die Person in die Weiterverarbeitung eingewilligt hat, nicht weitergibt. Es muss genau überprüft werden, ob die Erfolgsaussichten der Bewerbungen oder der weiteren Entwicklung im Arbeitsverhältnis tatsächlich nicht beeinträchtigt sind.

3. Für Trainingszwecke ist die Einwilligung aber keine rechtssichere Verarbeitungsgrundlage: Die betroffene Person kann ihre Einwilligung jederzeit widerrufen.[248] Das kann unter Umständen dazu führen, dass das ganze maschinell lernende System in der Form, wie es trainiert wurde, nicht mehr verwendet werden darf.

VI. Erforderlichkeit der Verarbeitung aufgrund berechtigter Interessen gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO

Es ist auch rechtmäßig, personenbezogene Daten zu Trainingszwecken maschinell lernender Systeme zu verarbeiten, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, dürfen allerdings das Interesse der Verantwortlichen an der Verarbeitung nicht überwiegen. Ob diese Voraussetzungen des Art. 6 Abs. 1 S. 1 lit. f

[248] Kapitel 6 B.V.3. (S. 151).

vorliegen, ist mithin mithilfe einer dreistufigen Prüfung zu ermitteln:[249] Zum Zeitpunkt der Verarbeitung muss ein berechtigtes Interesse des Verantwortlichen oder eines Dritten vorliegen. Die Datenverarbeitung muss erforderlich sein. Schließlich dürfen keine Grundrechte oder Grundfreiheiten der betroffenen Personen das Interesse an der Datenverarbeitung überwiegen. Die betroffene Person kann jederzeit aus Gründen, die sich aus ihrer besonderen Situation ergeben, der Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 S. 1 lit. f DSGVO erfolgt, gem. Art. 21 Abs. 1 DSGVO widersprechen.

1. Vorliegen berechtigter Interessen

Die Arbeitgeberin möchte durch den Einsatz maschinell lernender Systeme in ihrem Betrieb, Unternehmen oder Konzern schnellere und gerechtere Entscheidungen treffen, die keinen hohen Personaleinsatz erfordern. Diese Interessen sind „berechtigt" i. S. d. Art. 6 Abs. 1 S. 1 lit. f DSGVO.[250]

2. Erforderlichkeit des Trainings maschinell lernender Systeme mit personenbezogenen Daten

Die Verarbeitung personenbezogener Daten zu Trainingszwecken eines maschinell lernenden Systems ist nicht erforderlich, wenn ein gleich geeignetes, milderes Mittel zur Verfügung steht. Anonymisierte Daten als Trainingsdaten zu verwenden, ist ein milderes Mittel gegenüber der Verarbeitung personenbezogener Daten.[251] Allerdings ist es – wie ausgeführt worden ist – nicht unbedingt ein gleich geeignetes Mittel, wenn man anstelle von personenbezogenen Daten anonymisierte Daten verarbeitet. [252] Möglicherweise ist die Pseudonymisierung ein gleich geeignetes milderes Mittel.

---

[249] ErfK/*Franzen*, § 26 BDSG Rn. 5; Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 146; *Herfurth*, ZD 2018, 514.

[250] Zu den berechtigten Interessen i. S. d. Art. 6 Abs. 1 S. 1 lit. f DSGVO s. Kapitel 6 B.II.3.a)bb) (S. 124).

[251] S. dazu unter: Kapitel 6 B.II. (S. 121)

[252] S. dazu bereits unter: Kapitel 6 B.I. (S. 118).

a) Pseudonymisierung als milderes, gleich geeignetes Mittel

Gem. Art. 4 Nr. 5 DSGVO sind Daten pseudonymisiert, wenn sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.[253] Sie gelten weiterhin als personenbezogene Daten.

aa) Relativer oder absoluter Personenbezug

Entscheidend ist, ob es bei der Beurteilung, ob Personenbezug vorliegt, auf die Fähigkeiten und Möglichkeiten der jeweils verantwortlichen Stelle ankommt (sog. relativer Personenbezug) oder ob es ausreicht, dass irgendeine dritte Person Personenbezug herstellen kann (sog. absoluter Personenbezug).[254] Erwägungsgrund 26 DSGVO ist dahingehend offen und lässt beide Ansätze zu: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden [...]."

In der Rechtssache *Breyer* hat der EuGH sich zur aufgeworfenen Frage erstmals im Hinblick auf dynamische IP-Adressen geäußert.[255] Bei einer dynamischen IP-Adresse handelt es sich um eine IP-Adresse, die sich bei jeder neuen Internetverbindung ändert.[256] Den Rechnern wird bei jeder Sitzung eine gerade freie IP-Adresse aus einem Pool von IP-Adressen zugewiesen.[257] Nach außen tritt eine Nutzerin so bei jeder neuen Internetverbindung unter

---

[253] S. zu Abgrenzung Pseudonymisierung und Anonymisierung bereits unter: Kapitel 6 B.II.1.; zu Pseudonymisierungsverfahren s. *Schwartmann/Weiß*, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, 2017, S. 17 ff.

[254] Gola/Heckmann/*Pötters*, Art. 89 DSGVO Rn. 13, der das absolute Verständnis als überholt betrachtet; *Roßnagel*, ZD 2018, 243, 245; umfassend dazu s. *Mühlenbeck*, Anonyme und pseudonyme Daten, 2022, S. 106 ff.

[255] EuGH, 19.10.2016 – C-582/14, *Patrick Breyer ./. Bundesrepublik Deutschland*, ZD 2017, 24 (m. Anm. Kühling/Klar).

[256] EuGH, 19.10.2016 – C-582/14, *Patrick Breyer ./. Bundesrepublik Deutschland*, ZD 2017, 24, 25.

[257] Hoeren/Sieber/Holznagel, MultimediaR-Hdb/*Schmitz*, Teil 16.2. B. III. 1. Rn. 70.

einer anderen IP-Adresse auf.[258] Nur für die zuweisende Stelle weist die Adresse einen Bezug zu einer bestimmten Person auf. Der EuGH hatte die Frage zu beantworten, ob die dynamische IP-Adresse für den Webseitenbetreiber, der die direkte Zuordnung nicht kennt, Personenbezug hat.[259] Im Urteil entschied der EuGH, dass eine dynamische IP-Adresse für die Webseitenbetreiberin ein personenbezogenes Datum sei, „wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die die Internetzugangsanbieterin dieser Person verfügt, bestimmen zu lassen“[260]. Der EuGH hat sich somit für das relative Verständnis ausgesprochen. Dieses Verständnis hat der EuGH auch jüngst in einer Entscheidung bestätigt, in der es um die Fahrzeugidentifikationsnummer (FIN) ging.[261]

Das überzeugt. Ein absolutes Verständnis würde dazu führen, dass jede Art von Information als personenbezogenes Datum einzuordnen wäre.[262] Hinzu kommt, dass man – wenn man ein absolutes Verständnis zugrunde legt – faktisch nicht mehr zwischen Anonymisierung und Pseudonymisierung unterscheiden könnte. Sind die Daten anonymisiert, ist der Personenbezug entfernt. Wenn niemand die Daten entschlüsseln kann, sind sie i. E. anonymisiert und nicht nur pseudonymisiert. Die Pseudonymisierung wirkt dann anonymisierend.[263] Entscheidend ist daher, ob die verantwortliche Person den Schlüssel hat oder erhalten kann, der das Individuum identifiziert oder identifizierbar macht.

bb) Mittel zur Identifizierung

Bei der Frage, ob bestimmte Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden

---

[258] Hoeren/Sieber/Holznagel, MultimediaR-Hdb/*ders.*, Teil 16.2 B. III. 1. Rn. 70.

[259] Hoeren/Sieber/Holznagel, MultimediaR-Hdb/*ders.*, Teil 16.2 B. III 1. Rn. 70.

[260] EuGH, 19.10.2016 – C-582/14, *Patrick Breyer ./. Bundesrepublik Deutschland*, ZD 2017, 24, 26.

[261] EuGH, 09.11.2023 – C-319/22, *Gesamtverband Autoteile-Handel e.V. ./. Scanica CV AB*, juris, Rn. 48.

[262] GA Sánchez Bordona, Schlussantrag in der Rs. EuGH, 12.5.2016 – C-582/14, BeckRS 2016, 81027, Rn. 65.

[263] S. dazu bereits unter: Kapitel 6 B.II.2. (S. 122).

sollen, sollten gem. Erwägungsgrund 26 S. 3 DSGVO objektive Faktoren wie Kosten der Identifizierung und der erforderliche Zeitaufwand berücksichtigt werden.

Das erfordert eine umfassende Einzelfallbetrachtung und ist je nach Unternehmensgröße und Kontakten zu Personen mit (Sonder-)Wissen gesondert zu beurteilen. Wichtig ist zudem, dass die Verantwortlichen die Prüfung nicht nur einmalig vornehmen, sondern periodisch neu evaluieren, da sich die Zugänglichkeit zu technischen Mitteln, die ggf. zu einer Identifizierung führen, ständig ändert.[264]

Erwägungsgrund 26 S. 3 DSGVO erwähnt nicht, ob die genutzten Mittel legal sein müssen. In der Rechtssache *Breyer* hat der EuGH entschieden, dass verbotene Mittel außer Betracht bleiben.[265] Dieser Ansicht wird in der Literatur vereinzelt zugestimmt.[266] Im Ergebnis überzeugt es aber nicht, dass illegale Mittel zur Re-Identifizierung unberücksichtigt bleiben.[267] Die betroffenen Personen sind gerade besonders schutzwürdig, wenn es mit illegalen Mitteln *möglich* wäre, den Personenbezug wiederherzustellen.[268] Würde man in solchen Fällen die illegalen Mittel nicht berücksichtigen, widerspräche das dem Zweck der DSGVO, personenbezogene Daten zu schützen.[269]

cc) Rechtsfolge der Pseudonymisierung

Werden personenbezogene Daten pseudonymisiert, können die Risiken der betroffenen Person gesenkt werden und die Auftragsverarbeiterinnen bei

---

[264] Vgl. *Aichroth/Battis/Dewes*, Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens, 2020, S. 51.

[265] EuGH, 19.10.2016 – C-582/14, *Patrick Breyer ./. Bundesrepublik Deutschland*, ZD 2017, 24, 26 Rn. 46.

[266] *Kring/Marosi*, K&R 2016, 773, 775; *Mantz/Spittka*, NJW 2016, 3579, 3582.

[267] *Bergt*, ZD 2015, 365, 370; *Hacker*, Datenprivatrecht, 2020, S. 109.

[268] *Hacker*, Datenprivatrecht, 2020, S. 109; Kühling/Buchner/*Klar/Kühling*, Art. 4 DSGVO Rn. 29.

[269] *Hacker*, Datenprivatrecht, 2020, S. 109; Kühling/Buchner/*Klar/Kühling*, Art. 4 DSGVO Rn. 29.

der Einhaltung ihrer Datenschutzpflichten unterstützt werden.[270] Die pseudonymisierten Daten sind weiterhin personenbezogene Daten, jedoch werden die Grundrechte, d. h. das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG auf nationaler und das Datenschutzgrundrecht aus Art. 7, 8 GRCh auf unionaler Ebene der betroffenen Person durch die Pseudonymisierung weniger gefährdet.[271] Dieser Schutz greift auch dann, wenn die Pseudonymisierung nicht anonymisierend wirkt; denn auch da sind die Daten und der Schüssel, d. h. das zusätzliche Wissen, das die Identifizierung ermöglicht, voneinander getrennt.[272]

Für die Verantwortlichen führt die Verarbeitung pseudonymisierter Daten dazu, dass die Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO eher zu ihren Gunsten ausfällt.[273]

b) Ergebnis: Pseudonymisierung als milderes Mittel

Die Pseudonymisierung ist eine Möglichkeit, die hochsensiblen Daten einigermaßen zu schützen und gleichzeitig die Daten weiterhin zu nutzen.[274] Sie ist ein milderes und dabei doch gleich geeignetes Mittel gegenüber der Verarbeitung personenbezogener Daten in Reinform. Für die Verantwortliche ist es somit faktisch verpflichtend, soweit es möglich ist, pseudonymisierte Daten zu verwenden.[275] Zwar ist in der DSGVO nicht normiert, dass es rechtlich verpflichtend ist, pseudonymisierte Daten zu verarbeiten. Allerdings wird die Verarbeitung häufig erst rechtmäßig, wenn pseudonymisierte Daten verarbeitet werden. Mit pseudonymisierten Daten wird Art. 5 Abs. 1 lit. c DSGVO umgesetzt.[276]

---

[270] Erwägungsgrund 28 S. 1 DSGVO.

[271] *Roßnagel*, ZD 2018, 243, 245 f.

[272] *Ders.*, ZD 2018, 243, 245.

[273] *Ders.*, ZD 2018, 243, 246.

[274] *Aichroth/Battis/Dewes*, Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens, 2020, S. 18.

[275] Vgl. Sydow/Marsch/*Ziebarth*, Art. 4 DSGVO Rn. 105; *Mühlenbeck*, Anonyme und pseudonyme Daten, 2022, S. 363.

[276] *Mühlenbeck*, Anonyme und pseudonyme Daten, 2022, S. 363.

Eine rechtliche Verpflichtung, die Daten zu pseudonymisieren, ergibt sich bei bestimmten Verarbeitungssituationen: Etwa sieht Art. 10 Abs. 5 lit. b KI-VO-PARL vor, dass besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO für Hochrisiko-KI-Systeme pseudonymisiert verarbeitet werden dürfen, wenn es erforderlich ist, Verzerrungen aufzudecken und zu korrigieren.[277]

Für die Frage, ob Pseudonymisierung im Rechtssinn vorliegt, ist entscheidend, welche Mittel zur Verfügung stehen, um die Person zu identifizieren. Es ist angesichts der schnellen technischen Entwicklung nahezu unmöglich, immer alle technischen Neuerungen zu berücksichtigen, sodass es auch möglich ist, dass eine bestimmte Identifizierungsmöglichkeit unberücksichtigt bleibt. Für die Frage der Erforderlichkeit muss aber auch nicht zwingend Pseudonymisierung im Rechtsinn vorliegen, vielmehr müssen nur alle möglichen technischen Maßnahmen getroffen werden, um einen größtmöglichen Schutz für die personenbezogenen Daten zu ermöglichen.

3. Kein Entgegenstehen überwiegender Interessen der betroffenen Person

Den berechtigten Interessen der Verantwortlichen dürfen keine überwiegenden Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person entgegenstehen. Wenn Rechte der betroffenen Person tangiert werden, ist die Datenverarbeitung aber nicht bereits deshalb unzulässig. [278] Grundsätzlich garantiert das Datenschutzgrundrecht gem. Art. 7, 8 GRCh, das durch die DSGVO konkretisiert wird, unter anderem über die Verwendung der eigenen Daten selbst zu entscheiden.[279] Anders als bei der Abwägung im Hinblick auf eine Anonymisierung der Daten [280], überwiegen beim Training mit pseudonymisierten Daten, sofern diese gleich geeignet sind, nicht von vorneherein die Interessen der Verantwortlichen. Schließlich besteht das Risiko, dass die Daten der betroffenen Person entschlüsselt werden. Das wiederum fällt in den Risikobereich der Verantwortlichen, die gem. Art. 24 Abs. 1 S. 1 DSGVO auch die

---

[277] S. Kapitel 11 B. (S. 371 ff.).
[278] Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 62.
[279] Kapitel 5 A.II.3.a) (S. 60).
[280] Kapitel 6 B.II.3.a)dd) (S. 126).

hinreichenden technischen organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten treffen muss.

Für ein Überwiegen der Interessen der Verantwortlichen an der Datenverarbeitung spricht aber folgende Erwägung: Wie bereits ausgeführt worden ist[281], ist ein maschinell lernendes System nach dem Training grundsätzlich nicht mehr personenbezogen. Allerdings ist es möglich, etwa mit Kenntnis bestimmter Daten Rückschlüssen auf die *Input-Daten* zu erhalten.[282] Mithilfe geeigneter Vorkehrungen ist es aber erreichbar, das Risiko zu minimieren, sodass man keine Rückschlüsse auf die personenbezogenen *Input-Daten* erhält.[283] Trifft man derartige angemessenen Vorkehrungen, spricht das eher dafür, dass die Interessen der Verantwortlichen an der Datenverarbeitung überwiegen. Das Ergebnis der Abwägung i. S. d. Art. 6 Abs. 1 S. 1 lit. f. DSGVO hängt somit auch maßgeblich von den technischen Vorkehrungen ab, die die Verantwortliche trifft.

4. Zwischenergebnis zum Training gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO

1. Verarbeitet man die personenbezogenen Daten zu Trainingszwecken auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f DSGVO, ist die Verarbeitung erforderlich, wenn die Daten pseudonymisiert verarbeitet werden. Die Verarbeitung pseudonymisierter Daten ist gegenüber der Verarbeitung personenbezogener Daten ein milderes Mittel.[284]

2. Für die Verantwortliche besteht faktisch eine Pflicht, die Daten zu pseudonymisieren. Durch die Pseudonymisierung wird die Verarbeitung erst rechtmäßig. Eine direkte Pflicht zur Pseudonymisierung normiert etwa Art. 10 Abs. 5 lit. b KI-VO-PARL.[285]

---

[281] Kapitel 6 B.IV.4.e) (S. 142).
[282] Kapitel 6 B.IV.4.e) (S. 142).
[283] Kapitel 6 B.IV.4.e) (S. 142).
[284] Kapitel 6 B.VI.2.a) (S. 155).
[285] Kapitel 11 B. (S. 371 ff.)

3. Außerdem dürfen die Interessen der betroffenen Personen nicht überwiegen. Die Interessen der betroffenen Personen überwiegen dann nicht, wenn geeignete Schutzmaßnahmen für die relevanten Daten getroffen wurden: Wie auch bereits im Rahmen von Art. 6 Abs. 4 DSGVO hängt das Ergebnis der Abwägung nach Art. 6 Abs. 1 lit. f. DSGVO ebenfalls maßgeblich von den technischen Vorkehrungen ab, die die Verantwortliche trifft.[286]

C. Einsatz algorithmischer Systeme im Arbeitsverhältnis

Seit dem Urteil des EuGH vom 30. März 2023[287] kann man nicht mehr auf § 26 Abs. 1 S. 1 BDSG als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext zurückgreifen. [288] Werden algorithmische Systeme im Arbeitsverhältnis eingesetzt, kommen als mögliche Rechtsgrundlage daher Art. 6 Abs. 1 S. 1 lit. b DSGVO sowie die Einwilligung gem. § 26 Abs. 2 BDSG i. V. m. Art. 4 Nr. 11, 6 Abs. 1 S. 1 lit. a, 7 Abs. 4 DSGVO Betracht.

Bevor auf die Voraussetzungen der Einwilligung gem. § 26 Abs. 2 BDSG i. V. m. Art. 4 Nr. 11, 6 Abs. 1 S. 1 lit. a, 7 Abs. 4 DSGVO eingegangen wird, muss zunächst der Anwendungsbereich von § 26 BDSG in sachlicher und persönlicher Hinsicht eröffnet sein.

I. Sachlicher Anwendungsbereich von § 26 BDSG

Der sachliche Anwendungsbereich der Norm ist eröffnet, wenn personenbezogene Daten von Beschäftigen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden.

---

[286] Kapitel 6 B.VI.3. (S. 159).

[287] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[288] Kapitel 5 B.II.1.c) (S. 92).

1. Verarbeitung personenbezogener Daten

Personenbezogene Daten i. S. d. § 26 BDSG werden genauso definiert wie im Anwendungsbereich der DSGVO.[289] Insofern ist auf die vorherigen Ausführungen zu verweisen.[290]

Werden Bewerberinnendaten oder Daten einzelner Arbeitnehmerinnen durch ein algorithmisches System verarbeitet, wird es sich dabei stets um Daten handeln, die sich auf eine identifizierbare Person beziehen. Personenbezogene Daten liegen daher vor, sodass der sachliche Anwendungsbereich in dieser Hinsicht eröffnet ist.

2. Zwecke des Beschäftigungsverhältnisses

Die Verarbeitung muss für „Zwecke des Beschäftigungsverhältnisses" erfolgen. Der Verarbeitungszweck muss mithin im Zusammenhang mit einem beabsichtigten, bestehenden oder beendeten Beschäftigungsverhältnis stehen.[291] Werden Daten im Bewerbungsstadium oder im bestehenden Arbeitsverhältnis verarbeitet, wird die Verarbeitung meistens Zwecken des Beschäftigungsverhältnisses dienen. Dient die Verarbeitung anderen Zwecken und nicht vorrangig dem Beschäftigungsverhältnis, ist § 26 BDSG nicht einschlägig und es muss auf eine andere Rechtsgrundlage für die Verarbeitung personenbezogener Daten zurückgegriffen werden. Etwa kann bei anderen Zwecken als denen des Beschäftigungsverhältnisses auch Art. 6 Abs. 1 S. 1 lit. f DSGVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten herangezogen werden.[292]

3. Nicht automatisierte Verarbeitung auch erfasst

Vom sachlichen Anwendungsbereich ist nach § 26 Abs. 7 BDSG jede Art der Verarbeitung von Beschäftigtendaten erfasst: Die Absätze 1-6 gelten auch, wenn Daten nicht in einem Dateisystem gespeichert sind oder gespeichert

---

[289] Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 4.

[290] Kapitel 5 A.III.2.a)aa) (S. 65).

[291] Sydow/Marsch/*Tiedemann*, § 26 BDSG Rn. 19.

[292] S. Kapitel 6 A.II.2.b) (S. 108); so auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 224.

werden sollen. Der Verarbeitungsbegriff unterscheidet sich somit nicht von dem Verarbeitungsbegriff der DSGVO (Art. 4 Nr. 2 DSGVO). Diese Ausnahme wird für den Untersuchungsgegenstand indes nicht relevant sein. Werden Daten mittels eines algorithmischen Systems verarbeitet, handelt es sich stets um eine automatisierte Verarbeitung.

II. Persönlicher Anwendungsbereich

In persönlicher Hinsicht ist § 26 BDSG auf Beschäftigte anwendbar. Der Begriff der Beschäftigten ist in § 26 Abs. 8 BDSG bestimmt. Nach § 26 Abs. 1 S. 1 BDSG sind insbesondere Arbeitnehmerinnen einschließlich Leiharbeitnehmerinnen, Auszubildende, Rehabilitandinnen, Beschäftigte in Behindertenwerkstätten, Freiwilligendienstleistende, arbeitnehmerähnliche Personen und Beamtinnen umfasst. Gem. § 26 Abs. 8 S. 2 BDSG gelten auch Bewerberinnen für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, als Beschäftigte. Der weite persönliche Anwendungsbereich wird für Arbeitnehmerinnen und Bewerberinnen, deren Daten mittels algorithmischer Systeme verarbeitet wird, stets eröffnet sein.

III. § 26 Abs. 2 BDSG: Einwilligung

Soll für den Abschluss eines konkreten Arbeitsverhältnisses ein algorithmisches System eingesetzt werden, ist – wenn die Einwilligung als Rechtsgrundlage gewählt wird – § 26 Abs. 2 BDSG maßgeblich. Die Vorgaben der Art. 4 Nr. 11, 6 Abs. 1 S. 1 lit. a sowie 7 DSGVO gelten auch im Rahmen des § 26 Abs. 2 BDSG.[293]

1. Zentrales Merkmal: Freiwilligkeit

Zentrales Merkmal der Einwilligung i. S. d. § 26 Abs. 2 BDSG ist wie auch schon bei Art. 6 Abs. 1 S. 1 lit. a DSGVO, dass sie *freiwillig* erfolgen muss. Gem. § 26 Abs. 2 S. 1 BDSG sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende

---

[293] *Meinecke*, Datenschutz und Data Science, 2021, S. 147; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 206.

Abhängigkeit der beschäftigten Person sowie die Umstände zu berücksichtigen, unter denen die Einwilligung erteilt worden ist.

a) Freiwilligkeit im Bewerbungsstadium oder Arbeitsverhältnis

Viele Stimmen in der Literatur sprechen sich dafür aus, dass Freiwilligkeit im Arbeitsverhältnis faktisch ausgeschlossen sei.[294]

Im Bewerbungsstadium sei die Freiwilligkeit besonders problematisch: Möchte jemand die Zusage für eine bestimmte Stelle erhalten, bestehe die Gefahr, dass die Person aufgrund der Drucksituation in die Datenverarbeitung einwillige. Schließlich fürchte sie, die Stelle ansonsten nicht zu erhalten.[295] Das Arbeitsverhältnis bilde die soziale und wirtschaftliche Existenzgrundlage einer Arbeitnehmerin; sie sei auf den Arbeitsplatz angewiesen.[296]

Andere Stimmen möchten die Freiwilligkeit nicht pauschal ablehnen. Die Einwilligung drücke die informationelle Selbstbestimmung aus.[297] Eine betroffene Person könne selbst entscheiden, ob ihre personenbezogenen Daten verarbeitet würden oder nicht. Daher sei es nicht überzeugend,

---

[294] Vgl. Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 63; *Blum*, People Analytics, 2021, S. 113; differenzierter: *Götz*, Big Data im Personalmanagement, 2020, S. 55 ff.; *Meinecke*, Datenschutz und Data Science, 2021, S. 150 ff.; *Ernst*, ZD 2017, 110, 112; ablehnend jedenfalls bei einer kommerziellen Nutzung der Daten: *Simitis*, in: Hanau/Heither/Kühling (Hrsg.), Richterliches Arbeitsrecht: Festschrift für Thomas Dieterich zum 65. Geburtstag, 1999, S. 601, 623.

[295] *Folkerts*, DuD 2022, 77, 78; vgl. *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2015, S. 127.

[296] *BT-Drs. 18/11325*, S. 97; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018, S. 167; *Oberthür*, in: Kramer (Hrsg.), Kramer IT-ArbR, 2019, B. XI. 1. b) Rn. 881; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2015, S. 22 f.; *Schwarze*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 8 Rn. 8.

[297] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 206 m. w. N.; *Tinnefeld/Conrad*, ZD 2018, 391.

grundsätzlich eher von einer Unfreiwilligkeit auszugehen, wenn es sich um ein Bewerbungsverhältnis oder Arbeitsverhältnis handele.[298]

Das BAG hat in einem Urteil von 2016 sogar eine Einwilligung in eine Videoüberwachung als zulässig angesehen:[299] Obwohl ein schwerer Eingriff in das Persönlichkeitsrecht wegen des permanenten Überwachungsdrucks vorgelegen habe, sei der Eingriff durch die Einwilligung gedeckt gewesen.[300] Der Zweite Senat führte in seinem Urteil aber nicht näher aus, welche Anforderungen an das Merkmal der Freiwilligkeit gestellt werden und wie sie im vorliegenden Fall relevant waren.

Hinsichtlich der Umstände, die relevant für die Beurteilung der Freiwilligkeit sind, ist *Folkerts* zuzustimmen: Es muss insbesondere darauf geachtet werden, dass (1) die Einwilligung nicht aus einer konkreten Drucksituation rührt, (2) ein anderer Beweggrund außer der Druckausübung für die Einwilligung erkennbar ist und (3) die Einwilligung abgelehnt werden kann, ohne dass Nachteile drohen.[301] Um zu beurteilen, ob eine Drucksituation vorliegt, kann auch der Zeitpunkt maßgebend sein, in dem die Einwilligung erteilt wird.[302] Wird die Einwilligung vor Abschluss des Arbeitsvertrags oder im bestehenden Arbeitsverhältnis erteilt? Die Drucksituation wird zumeist vor Abschluss des Arbeitsvertrags größer sein.[303] Die Annahme, im Bewerbungsstadium bestehe stets eine noch größere Drucksituation aufgrund der Abhängigkeit, ist jedoch nicht immer gerechtfertigt: Je nach Branche werden (gut) qualifizierte Arbeitnehmerinnen händeringend gesucht. [304] Gut qualifizierte Arbeitnehmerinnen haben deshalb eine große Auswahl an verschiedenen Arbeitgeberinnen, sodass sie aufgrund der für sie positiven Marktsituation häufig nicht darauf angewiesen sind, eine bestimmte Stelle anzunehmen.

---

[298] Taeger/Gabel/*Taeger*, Art. 7 DSGVO Rn. 105; *Hacker*, Datenprivatrecht, 2020, S. 195; *Folkerts*, DuD 2022, 77, 79.

[299] BAG, 20.10.2016 – 2 AZR 395/15, NZA 2017, 444.

[300] BAG, 20.10.2016 – 2 AZR 395/15, NZA 2017, 444, 447.

[301] *Folkerts*, DuD 2022, 77, 78 f.

[302] *BT-Drs. 18/11325*, S. 97.

[303] *Ebd.*, S. 97.

[304] Ifo Institut, Umfrage zum Fachkräftemangel unter Dienstleistern nach Branchen in Deutschland 2022, Statista, s. https://perma.cc/EPV8-2BVB (archiviert am 18.10.2022).

Problematisch ist im Bewerbungsstadium außerdem das Rechnungstragungsgebot nach Art. 7 Nr. 4 DSGVO.[305] Zwar normiert das Gebot kein Kopplungsverbot in dem Sinn, dass die Einwilligung in eine Datenverarbeitung niemals an eine Vertragserfüllung geknüpft werden kann. Etwa ist es zulässig, die konkrete Leistungserbringung von der Einwilligung in die Datenverarbeitung abhängig zu machen, wenn die Datenverarbeitung die „notwendige Entscheidungs- oder Kalkulationsgrundlage für das konkrete Rechtsgeschäft darstellt“[306]. Die Arbeitgeberin kann daher von der Kenntnis über die Qualifikation ihrer Bewerberin die Einstellung abhängig machen; vorleistungspflichtige Unternehmen können eine Leistung von der Bonität der Kundinnen abhängig machen.[307] Es ist aber nicht möglich, die Datenverarbeitung mittels algorithmischer Systeme davon abhängig zu machen, ob ein Arbeitsverhältnis überhaupt begründet wird. Das widerspricht nicht nur Art. 7 Abs. 4 DSGVO, sondern schließt auch eine Freiwilligkeit aus, weil eine Wahlmöglichkeit nicht mehr besteht: Wenn die Datenverarbeitung für die Begründung des Arbeitsverhältnisses *erforderlich* ist, bleibt für einen echte Wahlmöglichkeit und somit eine Einwilligung kein Spielraum.[308]

b) Vorteil oder gleichgelagerte Interessen i. S. d. § 26 Abs. 2 S. 2 BDSG

Freiwilligkeit kann nach § 26 Abs. 2 S. 2 BDSG insbesondere vorliegen, „wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeberin und beschäftigte Person gleichgelagerte Interessen verfolgen“. Ein derartiger Vorteil wird etwa darin gesehen, wenn ein betriebliches Gesundheitsmanagementsystem zur Gesundheitsförderung eingeführt werden soll oder die Einwilligung dazu dient, dass betriebliche IT-Systeme auch privat genutzt werden dürfen.[309] Gleichgelagerte Interessen

---

[305] Kapitel 6 B.V.2.b) (S. 147).

[306] Kühling/Buchner/*Buchner/Kühling*, Art. 7 DSGVO Rn. 47.

[307] BGH, 21.3.2003 – III ZR 54/02, NJW 2003, 1237-1241, 1240; Kühling/Buchner/*dies.*, Art. 7 DSGVO Rn. 47.

[308] Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 203; Kühling/Buchner/*Maschmann*, Art. 88 DSGVO Rn. 51;

[309] *BT-Drs. 18/11325*, S. 97.

liegen z. B. vor, wenn Name und Geburtsdatum in eine Geburtstagsliste eingetragen werden oder Fotos im Intranet veröffentlicht werden.[310]

Ein solcher eindeutiger Vorteil liegt nicht vor, wenn die Bewerberin in die Datenverarbeitung durch ein algorithmisches System einwilligt: Die Chancen, die Zusage für die Stelle zu erhalten, werden durch den Einsatz eines solchen Systems nicht erhöht. Zwar kann man argumentieren, dass die Entscheidung eines algorithmischen Systems gegenüber menschlichen Entscheidungen objektiv ist.[311] Auch algorithmische Systeme können aber diskriminieren und unfaire Entscheidungen herbeiführen.[312] Etwas anderes kann sich aber ergeben, wenn im bestehenden Arbeitsverhältnis in eine derartige Datenverarbeitung eingewilligt wird, etwa um an einem internen Fortbildungsprogramm teilzunehmen, das sich positiv auf die Leistungsentwicklung der Arbeitnehmerinnen auswirkt. Wenn die Arbeitnehmerinnen nur davon profitieren und keine Nachteile für sie mit der Datenverarbeitung einhergehen, ist die Verarbeitung für sie vorteilhaft.

c) Folgen für die Praxis: Schwierige Beweisführung

Das Merkmal der Freiwilligkeit ist in der Praxis ein Problem der Beweislast. Die Arbeitgeberin muss beweisen, dass die Datenverarbeitung rechtmäßig war und somit auch beweisen, dass die Voraussetzungen einer wirksamen Einwilligung vorlagen. Sie ist die Verantwortliche der Datenverarbeitung und trägt mithin die Darlegungs- und Beweislast dafür, dass die Zulässigkeitsvoraussetzungen dafür vorliegen, dass sie die personenbezogenen Daten verarbeiten darf.[313] Es ist aber schwierig, nachzuweisen, dass die Kandidatinnen eine echte Wahlmöglichkeit hatten und nicht aufgrund einer Drucksituation, sondern aus anderen Gründen eingewilligt haben. Unternehmen, die Daten mittels algorithmischer Systeme auf Basis von

---

[310] *Ebd.*, S. 97.

[311] Kapitel 3 (S. 33).

[312] Kapitel 8 (S. 281).

[313] OLG Stuttgart 12. Zivilsenat, 18.5.2021 – 12 U 296/20, ZD 2022, 105; Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 7.

Einwilligungen verarbeiten[314], weisen zwar auf ihrer Website darauf hin, dass eine Nutzung der Software freiwillig ist und den Kandidatinnen kein Nachteil daraus entsteht, wenn sie das Tool nicht verwenden.[315] Die bloße Behauptung, den Kandidatinnen entstünde kein Nachteil, reicht aber nicht aus, um von einer echten Wahlmöglichkeit und Freiwilligkeit der Bewerberinnen auszugehen. [316] Vielmehr müssten die Unternehmen offenlegen, wie der Auswahlprozess sich mit und ohne Einwilligung in die Datenverarbeitung mittels algorithmischer Systeme gestaltet. Wenn danach erkennbar ist, dass tatsächlich keine Nachteile für die Bewerberinnen entstehen, besteht eine echte Wahlmöglichkeit und die Einwilligung kann freiwillig sein.

d) Zwischenergebnis: Hohe Anforderungen an das Merkmal der Freiwilligkeit

Die vorstehenden Ausführungen zeigen: Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, müssen alle Umstände des Einzelfalls in die Abwägung miteinbezogen werden. Der Zeitpunkt, wann die Einwilligung erteilt wird, der Anlass der Einwilligung und die damit womöglich bestehende Drucksituation sind Kriterien, die eine Rolle spielen.

Freiwilligkeit liegt nur vor, wenn die betroffene Person eine echte Wahlmöglichkeit hat.[317] Wenn im Bewerbungsstadium die Einwilligung in die Datenverarbeitung durch ein algorithmisches System erforderlich ist, um am weiteren Prozess teilzunehmen, schließt das eine freiwillige Einwilligung aus. Als Abwägungskriterium muss auch die individuelle Situation der Bewerberin miteinbezogen werden. Wenn die Bewerbung womöglich nur eine von vielen ist und die Person bereits Zusagen von anderen Arbeitgeberinnen erhalten hat oder ihre Position auf dem Arbeitsmarkt derart hervorsticht, kann eine

---

[314] S. hierzu beispielhaft das frühere Geschäftsmodell des Unternehmens *Retorio*: Datenschutzerklärung *Retorio* (Stand:06.2021), https://perma.cc/FZS5-467K (archiviert am 24.11.2022).

[315] https://perma.cc/M9AX-22V9 (archiviert am 02.08.2022).

[316] *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 170; kritisch dazu auch: *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2015, S. 126 f.

[317] Zur Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis s.: *Der Europäische Datenschutzausschuss* (EDSA), Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 2020, S. 10.

Einwilligung trotz des im Bewerbungsstadiums bestehenden Drucks freiwillig erteilt werden.[318] Es wird aber schwierig für die Arbeitgeberin sein, zu beweisen, dass die Einwilligung auch freiwillig erteilt wurde.

Eine andere Situation ergibt sich aber im bestehenden Arbeitsverhältnis, wenn der Arbeitnehmerin durch die Einwilligung ein Vorteil zugutekommt oder Arbeitgeberin und Arbeitnehmerin gleichgelagerte Interessen haben. Diese Voraussetzungen werden bei der Einwilligung in die Datenverarbeitung durch ein algorithmisches System zu individuellen Förderungszwecken in der Regel erfüllt sein.

2. Informiertheit der Einwilligung

Die betroffene Person muss vorab darüber informiert werden, welche Daten zu welchem Zweck von wem verarbeitet werden.[319] Das ist erforderlich, um die Einwilligung „in Kenntnis der Sachlage" abzugeben.[320] Wie die Information über die Verarbeitungszwecke und die Verantwortliche erfolgt, ist nicht gesetzlich definiert. Hier ist es wichtig, dass die Informationen so übersichtlich und verständlich wie möglich präsentiert werden. Der betroffenen Person muss bewusst sein, in welche Verarbeitung sie genau einwilligt.

Wie bereits im Kontext der Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO ausgeführt, muss beim Einsatz algorithmischer Systeme die betroffene Person nicht nur darüber informiert werden, welche Daten zu welchen Zwecken verarbeitet werden, sondern auch darüber, welche Risiken möglicherweise für sie mit dem Einsatz des algorithmischen Systems einhergehen.[321]

Zudem muss die betroffene Person gem. Art. 7 Abs. 3 S. 3 DSGVO über das Widerrufsrecht belehrt werden. Die Einwilligung kann nach Art. 7 Abs. 3 S. 1 DSGVO jederzeit widerrufen werden. Wie auch schon im Kontext von Art. 6

---

[318] S. dazu auch das Beispiel von *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 172 f.

[319] Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 8.

[320] Vgl. Erwägungsgrund 42 S. 4 DSGVO.

[321] Kapitel 6 B.V.2.d) (S. 150).

Abs. 1 S. 1 lit. a DSGVO[322] wirkt der Widerruf für die Zukunft. Die Daten dürfen nicht mehr für weitere Verarbeitungsprozesse genutzt werden. Je nachdem, ob Rückschlüsse auf die personenbezogenen Daten zulässig sind, müssen die entsprechenden Daten aus dem System gelöscht werden.[323]

3. Form

Die Einwilligung muss nicht ausdrücklich oder schriftlich erfolgen. Eine „eindeutig bestätigende Handlung" reicht aus.[324] Sog. „*Opt-out-Varianten*" sind unzulässig: [325] Erwägungsgrund 32 S. 3 DSGVO sieht vor, dass Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person nicht als Einwilligung gelten. Die verantwortliche Person muss nachweisen können, dass die Anforderungen an die Form gewahrt wurden.

4. Zwischenergebnis: Einwilligung ist keine taugliche Rechtsgrundlage

1. Bei der Einwilligung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist insbesondere das Merkmal der Freiwilligkeit problematisch. Bei der Begründung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis liegt eine freiwillige Einwilligung aber regelmäßig nur vor, wenn es um Vorteile für die betroffene Person geht oder die Verantwortliche und betroffene Person gleichgelagerte Interessen haben.[326]

2. Die Einwilligung kann außerdem jederzeit widerrufen werden, sodass die Verarbeitungsgrundlage *ex nunc* entfällt und die Daten gem. Art. 17 Abs. 1 lit. b DSGVO gelöscht werden müssen. Anders als beim Training algorithmischer Systeme kommt es nicht zum Problem, dass das verarbeitete Datum gewissermaßen Bestandteil des Algorithmus

---

[322] Kapitel 6 B.IV.2. (S. 135).

[323] Dazu bereits unter: Kapitel 6 B.V.3. (S. 151).

[324] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 33; Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 11.

[325] BeckOK Datenschutzrecht/*Stemmer*, Art. 7 DSGVO Rn. 86; EuGH, 11.11.2020 – C-61/19, NJW 2021, 841, 843 Rn. 37.

[326] Kapitel 6 C.III.1.b) (S. 166).

geworden ist und ggf. das System in der Form nicht mehr eingesetzt werden kann.[327]

IV. Art. 6 Abs. 1 lit. b DSGVO als Verarbeitungsgrundlage im Beschäftigungskontext

1. Übertragbarkeit der Grundsätze zu § 26 Abs. 1 S. 1 BDSG auf Art. 6 Abs. 1 S. 1 lit. b DSGVO?

Seit dem Urteil des EuGH vom 30. März 2023[328] kann man auf § 26 Abs. 1 S. 1 BDSG als Verarbeitungsgrundlage im Beschäftigungskontext nicht mehr zurückgreifen.[329] Pendant zu § 26 Abs. 1 S. 1 BDSG ist Art. 6 Abs. 1 S. 1 lit. b DSGVO. Art. 6 Abs. 1 S. 1 lit. b DSGVO regelt, dass die Verarbeitung rechtmäßig ist, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zu Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Anders als § 26 Abs. 1 S. 1 BDSG ist Art. 6 Abs. 1 S. 1 lit. b DSGVO nicht auf den Beschäftigungskontext beschränkt. Anwendbar ist die Norm aber auch, wenn es um die Erfüllung eines Vertrags geht, sodass die Norm einen ähnlichen Regelungscharakter wie § 26 Abs. 1 S. 1 BDSG hat.

Das Unionsrecht ist autonom auszulegen.[330] Auch wenn Merkmale einer nationalen Norm gleichermaßen auch in einer Vorschrift des Unionsrechts enthalten sind, ist das inhaltliche Verständnis nicht zwingend gleich. Somit kann man nicht ohne Weiteres die Grundsätze des Merkmals „Durchführung des Beschäftigungsverhältnisses" gem. § 26 Abs. 1 S. 1 BDSG auf das Merkmal der „Erfüllung eines Vertrages" gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO übertragen.[331] Gleiches gilt bei dem Merkmal der „Erforderlichkeit". Unter dem Merkmal „Erfüllung eines Vertrags" kann aber jedenfalls das Bewerbungsverfahren gefasst werden. Ohne ein solches Bewerbungsverfahren

---

[327] S. hierzu bereits unter: Kapitel 6 B.V.3. (S. 151).

[328] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[329] Kapitel 5 B.II.1.c) (S. 92).

[330] St. Rspr.: EuGH, 21.10.2010 – C-467/08, juris, Rn. 32; Calliess/Ruffert/*Wegener*, Art. 19 EUV Rn. 28.

[331] *Wünschelbaum*, NZA 2023, 487, 545.

kann ein Arbeitsverhältnis nicht begründet werden. „Vertrag" i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO erfasst jedenfalls rechtsgeschäftliche Schuldverhältnisse wie das Arbeitsverhältnis.[332]

Bei dem Merkmal der „Erforderlichkeit" muss gesondert geprüft werden, welche Kriterien i. R. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO relevant sind. Die folgenden Ausführungen setzen sich daher damit auseinander, wie das Merkmal der Erforderlichkeit i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO verstanden wird und inwiefern man die Grundsätze zur Auslegung des Merkmals der Erforderlichkeit gem. § 26 Abs. 1 S. 1 BDSG übertragen kann.

2. Erforderlichkeit der Verarbeitung gem. § 26 Abs. 1 S. 1 BDSG und Art. 6 Abs. 1 S. 1 lit. b DSGVO

Personenbezogene Beschäftigtendaten dürfen gem. § 26 Abs. 1 S. 1 BDSG verarbeitet werden, soweit die Verarbeitung für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, nach Begründung oder für die Durchführung oder Beendigung erforderlich ist. Vorgängervorschrift von § 26 BDSG war § 32 BDSG a. F. Bereits im Wortlaut des § 32 BDSG a. F. war das Merkmal der Erforderlichkeit vorhanden. Das BAG hat i. R. d. § 32 Abs. 1 BDSG a. F. den Grundsatz der Verhältnismäßigkeit bei der Prüfung des Merkmals der Erforderlichkeit angewendet.[333] Für § 26 Abs. 1 S. 1 BDSG gilt dieser Grundsatz gleichermaßen.[334] Das bedeutet, dass die Datenverarbeitung dann erforderlich ist, wenn sie für den (zulässigen) Zweck geeignet ist und das mildeste aller effektiv zur Verfügung stehenden Mittel ist.[335] Außerdem muss die Verarbeitung auch verhältnismäßig im engeren Sinn (angemessen) sein.[336] Das ist dann der Fall, wenn die der Eingriff in die Persönlichkeitsrechte der

---

[332] BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 DSGVO Rn. 42.

[333] BAG, 20.6.2013 – 2 AZR 546/12, NZA 2014, 143, 146.

[334] Begr. RegE BT-Drs. 18/11325, S. 97; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 19; *Franzen*, ZfA 2019, 18, 34; *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 227 ff.

[335] BAG, 23.8.2018 – 2 AZR 133/18, NZA, 1329, 1332; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 19.

[336] BAG, 23.8.2018 – 2 AZR 133/18, NZA, 1329, 1332; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 19.

Arbeitnehmerin durch die Verarbeitung nicht außer Verhältnis zum Gewicht der rechtfertigenden Gründe steht.[337]

Es ist einzelfallabhängig, ob die Verarbeitung mithilfe eines algorithmischen Systems im Beschäftigungskontext erforderlich ist. Dennoch lassen sich allgemeine Erwägungen für die Datenverarbeitung mittels algorithmischer Systeme herausarbeiten, die im Rahmen der Erforderlichkeit i. S. d. § 26 Abs. 1 S. 1 BDSG relevant sind.

Demgegenüber wird „Erforderlichkeit" i. R. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO überwiegend so verstanden, dass die Verarbeitung für „die Erfüllung der konkreten Vertragszwecke notwendig und nicht nur nützlich ist".[338] Stimmen in der Literatur sprechen sich dafür aus, dass der Verhältnismäßigkeitsgrundsatz i. R. d. Art. 6 Abs. 1 lit. b DSGVO nicht berücksichtigt werden darf.[339] Im Privatrechtsverkehr finde der Verhältnismäßigkeitsgrundsatz keine Anwendung: Es sei überhöht, nur zwingend notwendige oder unverzichtbare Verarbeitungsvorgänge für erforderlich zu halten.[340]

Das überzeugt nicht. Die DSGVO konkretisiert Art. 7, 8 GRCh.[341] Auch wenn Reichweite, Umfang und Grenzen einer „mittelbaren Drittwirkung" der Grundrechte im Einzelnen unklar sind[342], bleiben Art. 7, 8 GRCh in Privatrechtsverhältnissen zu berücksichtigen, wenn die DSGVO ausgelegt

---

[337] BAG, 23.8.2018 – 2 AZR 133/18, NZA, 1329, 1332; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 19.

[338] Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 13; Gola/Heckmann/*Schulz*, Art. 6 DSGVO Rn. 38; Kühling/Buchner/*Buchner/Petri*, Art. 6 DSGVO Rn. 42 ff.; Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 57.

[339] Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 14; Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 57.

[340] Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 14; Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 57.

[341] S. Kapitel 5 A.III. (S. 61).

[342] S. dazu bereits: Kapitel 5 A.II.1.b) (S. 58); *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, Teil A. § 2 Rn. 64; *Fischer*, Die Horizontalwirkung der EU-Grundrechtecharta im Arbeitsrecht, 2023, S. 230 ff.

wird.[343] Art. 52 Abs. 1 S. 2 GRCh fordert, dass Einschränkungen der in der Charta anerkannten Rechte und Freiheiten nur unter Wahrung des Grundsatzes der Verhältnismäßigkeit vorgenommen werden dürfen. Die GRCh verlangt somit, dass die Verhältnismäßigkeit auch auf Ebene der DSGVO berücksichtigt wird.[344] Um dem Datenschutzgrundrecht gem. Art. 7, 8 GRCh hinreichend Rechnung zu tragen, muss daher im sich anbahnenden Arbeitsverhältnis und auch im laufenden Arbeitsverhältnis der Verhältnismäßigkeitsgrundsatz zum Tragen kommen. Es hat nicht zur Folge, dass nur „zwingend notwendige" oder „unverzichtbare" Verarbeitungsvorgänge möglich sind, wenn der Verhältnismäßigkeitsgrundsatz angewendet wird. Vielmehr muss gewährleistet sein, dass die Verarbeitung insgesamt verhältnismäßig ist.

Das Merkmal der Erforderlichkeit gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO ist daher – wie auch bereits im Rahmen von Art. 6 Abs. 1 S. 1 lit. f DSGVO[345] – als Ausprägung des Verhältnismäßigkeitsgrundsatzes zu verstehen.[346]

Der Unterschied zwischen der Prüfung des Merkmals der Erforderlichkeit i. S. d. § 26 Abs. 1 S. 1 BDSG und i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO ist somit gering, auch wenn es theoretisch Unterschiede zwischen der nationalen Verhältnismäßigkeitsprüfung und der unionsrechtlichen Verhältnismäßigkeitsprüfung geben kann.[347]

---

[343] Kapitel 5 A.II.1.b) (S. 58); s. umfassend dazu auch: *Fischer*, Die Horizontalwirkung der EU-Grundrechtecharta im Arbeitsrecht, 2023, S. 320.

[344] Vgl. HBDI, Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023 Rs. C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, S. 7, https://perma.cc/6ZR6-RQ7F (archiviert am 10.6.2023).

[345] Kapitel 6 B.II.3.a)cc) (S. 125).

[346] HBDI, Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023 Rs. C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, S. 7, https://perma.cc/6ZR6-RQ7F (archiviert am 10.6.2023).

[347] Zum unionalen Verhältnismäßigkeitsgrundsatz s. *Trstenjak/Beysen*, EuR 2012, 265; s. auch: *Glocker/Hoffmann*, BB 2023, 1333, 1335.

a) Kein generelles Verbot des Einsatzes algorithmischer Systeme

Im Jahr 1984[348] hat das BAG in Bezug auf graphologische Gutachten entschieden, die nach seiner Ansicht ohne Einwilligung des Betroffenen unzulässig waren. In diesem Urteil hat das BAG auch ausgeführt, dass die Verarbeitung personenbezogener Beschäftigtendaten mittels algorithmischer Systeme nicht bereits deshalb ausgeschlossen ist, weil es sich um ein Mittel handele, das „über jedermann zur Verfügung stehende Erkenntnismöglichkeiten [hinausgehe]"[349]. Grundsätzlich habe nämlich jeder frei darüber zu entscheiden, ob und inwieweit er das Ausleuchten der Persönlichkeit mit derartigen Mitteln gestatten wolle.[350] Diese Rechtsprechung dürfte angesichts der zunehmenden Digitalisierung überholt sein.[351] Im Jahr 2017 hat das BAG über den Einsatz von sog. *Keyloggern* entschieden.[352] Dabei handelt es sich um eine Software, die Tastatureingaben protokolliert und regelmäßig Screenshots fertigt. Eine solche Software ist eine Erkenntnismöglichkeit, die über die jedermann zur Verfügung stehende Möglichkeit hinausgeht. Zwar war im konkreten Fall der Einsatz unzulässig. Das BAG hat die Möglichkeit einer derartigen Überwachungsmaßnahme aber nicht grundsätzlich abgelehnt. Der Einsatz ist vielmehr an strenge Voraussetzungen geknüpft. Dem Urteil kann man aber entnehmen, dass solche Erkenntnismöglichkeiten unter bestimmten strengen Voraussetzungen eingesetzt werden können und nicht pauschal unzulässig sind.[353]

Der EuGH hat bislang noch nicht zu algorithmischen Systemen entschieden. Dass algorithmische Systeme nicht generell verboten sind, ergibt sich aber aus einem Umkehrschluss zu Art. 22 Abs. 1 DSGVO. Nach dieser Norm hat eine Person das Recht, nicht einer *ausschließlich* automatisierten Entscheidung unterworfen zu werden.[354] Grundsätzlich sind automatisierte Entscheidungen

---

[348] BAG, 16.9.1982 – 2 AZR 228/80, NJW 1984, 446.

[349] BAG, 16.9.1982 – 2 AZR 228/80, NJW 1984, 446.

[350] BAG, 16.9.1982 – 2 AZR 228/80, NJW 1984, 446.

[351] So auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 233.

[352] BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327-1332.

[353] Vgl. *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018, S. 156.

[354] Zu Art. 22 Abs. 1 DSGVO s. Kapitel 6 D. (S. 204).

aber nicht nach Art. 22 Abs. 1 DSGVO oder einer anderen Norm in der DSGVO untersagt. Auch auf unionaler Ebene existiert mithin kein generelles Verbot automatisierter Datenverarbeitung und algorithmischer Systeme.

b) Geeignetheit

Die Verarbeitung muss zunächst zur Erreichung eines legitimen Zwecks geeignet sein.[355] Das ist der Fall, wenn der angestrebte Zweck mit der Maßnahme der Arbeitgeberin gefördert wird.[356]

aa) Bedeutung der Qualität der Trainingsdaten

Ob ein maschinell lernendes System geeignet ist, unterstützend im Bewerbungsprozess oder im bestehenden Arbeitsverhältnis eingesetzt zu werden, hängt maßgeblich von der Qualität der Trainingsdaten ab.[357]

Das maschinell lernende System ist nämlich nicht geeignet, Bewerber- oder Mitarbeiterinnen für eine Beförderung vorzuschlagen, wenn Ergebnisse hervorgerufen werden, die für die jeweilige Person nicht zutreffen.[358] Maschinell lernende Systeme können z. B. Faktoren berücksichtigen, die mit der Qualifikation der Bewerberin nichts zu tun haben: Reporterinnen des BR haben eine Software zur Videoanalyse getestet, wobei herauskam, dass sich die KI von Faktoren wie Bildhintergrund oder Accessoires wie Brille, Kopftuch o. Ä. leiten lässt und zu unterschiedlichen Ergebnissen kommt.[359] Der Grund dafür, dass die KI sensibel auf bestimmte Merkmale reagiert, liegt darin, dass Verzerrungen in den Trainingsdaten durch das Training des Systems verstärkt werden: Wurden in den Trainingsdaten Personen häufig als „verlässlich" eingestuft und hatten sie ein Bücherregal im Hintergrund, kann der

---

[355] Sydow/Marsch/*Tiedemann*, § 26 BDSG Rn. 21.

[356] *Franzen*, ZfA 2019, 18, 33.

[357] *Dreyer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, S. 138; *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 53; vgl. *Neutatz/Abedjan*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 1.

[358] *Betz*, ZD 2019, 148, 149; vgl. dazu auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 230 f.

[359] S. https://perma.cc/8NUY-6399 (archiviert am 02.08.2022).

Algorithmus daraus eine Korrelation ableiten.[360] Zukünftig könnte das System solche Bewerberinnen als verlässlich einstufen, die ein Bücherregal im Hintergrund haben. Sucht die Arbeitgeberin vor allem nach Bewerberinnen, denen die Eigenschaft „verlässlich" zugeschrieben wird, würden demnach diejenigen Bewerberinnen einen Vorteil haben, die vor einem Bücherregal das Video aufgenommen haben. Mit ihrer Qualifikation hat das aber nichts zu tun.

Die Verantwortlichen müssen aktiv überprüfen, ob derartige sachfremde Erwägungen in die Entscheidung miteinfließen. Ist das der Fall, müssen sie Maßnahmen ergreifen, um durch sachfremde Erwägungen verfälschte Ergebnisse zu verhindern. Gelingt den Verantwortlichen das nicht, ist das algorithmische System bereits nicht geeignet, eine Entscheidung zu treffen.[361]

bb) Insbesondere: Wahrung des Fragerechts der Arbeitgeberin

Das algorithmische System ist zudem nur geeignet, das entsprechende Ziel zu fördern, etwa eine geeignete Bewerberin zu finden, solange es nur solche Informationen über die Person herausfindet, die zulässigerweise eingeholt werden dürfen, sog. Fragerecht der Arbeitgeberin.[362] Grundsätzlich sind bei einem Vorstellungsgespräch Fragen eher als unzulässig einzustufen, je mehr sie die Person betreffen und sich nicht auf die konkrete Stelle beziehen.[363] Bei Fragen, die für die angestrebte Tätigkeit bedeutungslos sind, steht den Bewerberinnen ein „Recht zur Lüge" zu.[364]

Ein direktes Pendant zum Fragerecht der Arbeitgeberin gibt es auf unionaler Ebene nicht. Der Schutzzweck des Fragrechts, nicht unzulässigerweise in das

---

[360] Vgl. https://perma.cc/LN3V-S8L5, Aussage Katharina Zweig, ab Minute 4 (archiviert am 02.08.2022); Kapitel 3 C

[361] Vgl. *Götz*, Big Data im Personalmanagement, 2020, S. 99, der darin einen Verstoß gegen den Richtigkeitsgrundsatz der DSGVO sieht.

[362] BAG, 20.3.2014 – 2 AZR 1071/21, NZA 2014, 1131, 1133 m. w. N.; *Asgari*, DB 2017, 1325, 1325 f.; *Kainer/Weber*, BB 2017, 2740, 2742.

[363] ErfK/*Franzen*, § 26 BDSG Rn. 13; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 29; *Joos*, NZA 2020, 1216, 1220.

[364] Zum Fragerecht der Arbeitgeberin s.: BAG, 20.3.2014 – 2 AZR 1071/21, NZA 2014, 1131; MüKoBGB/*Armbrüster*, § 123 Rn. 46 ff.; *Däubler*, NZA 2017, 1481.

Persönlichkeitsrecht der Arbeitnehmerinnen einzugreifen und die Individualsphäre zu wahren, greift aber auch im Unionsrecht. Dogmatisch kann man das Fragerecht der Arbeitgeberin in Art. 5 Abs. 1 lit. c DSGVO verorten.[365] Es würde dem Grundsatz der Datenminimierung widersprechen, wenn Informationen über die betroffene Person erhoben werden würden, die für die ausgeschriebene Stelle nicht zulässigerweise eingeholt werden dürfen. Dann wäre die Datenverarbeitung nicht gem. Art. 5 Abs. 1 lit. c DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt. Die dem nationalen Recht entnommenen Wertungen sollten daher auf das Unionsrecht übertragen werden.

c) Erforderlichkeit

Sind algorithmische Systeme geeignet, den jeweiligen Zweck zu fördern, muss der Einsatz des Systems auch erforderlich sein. Erforderlich im engeren Sinn ist die Verarbeitung personenbezogener Daten mittels eines algorithmischen Systems, wenn kein anderes gleich geeignetes, milderes Mittel zur Verfügung steht. [366] Gibt es ein milderes Mittel gegenüber der Datenverarbeitung mit einem algorithmischen System? Und wenn ja, ist es auch gleich geeignet?

aa) Mildere Mittel gegenüber einem algorithmischen System

Ein Mittel ist milder, wenn es gegenüber dem eingesetzten Mittel weniger eingriffsintensiv ist für die Grundrechte der betroffenen Personen. Die Erwägungen sind sowohl im Rahmen von § 26 Abs. 1 S. 1 BDSG als auch im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO gleichermaßen zu berücksichtigen. Während bei § 26 Abs. 1 S. 1 BDSG vor allem das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG[367] relevant ist, muss im Kontext von Art. 6 Abs. 1 S. 1 lit. b DSGVO das Datenschutzgrundrecht gem. Art. 7, 8 GRCh berücksichtigt werden.[368] Die Eingriffsintensität bestimmt sich nach verschiedenen Kriterien. Im Kontext

---

[365] Zu den Datenschutzgrundsätzen s. Kapitel 6 A.IV. (S. 114).

[366] Sydow/Marsch/*Tiedemann*, § 26 BDSG Rn. 22.

[367] S. Taeger/Gabel/*Zöll*, § 26 BDSG Rn. 25.

[368] S. Taeger/Gabel/*Taeger*, Art. 6 DSGVO Rn. 7.

von algorithmischen Systemen im Personalwesen müssen insbesondere folgende Punkte berücksichtigt werden: Wie eingriffsintensiv ist das eingesetzte Mittel für die relevanten Grundrechte der betroffenen Personen? Wie viele personenbezogene Daten gibt die Person preis? Welchen zeitlichen Aufwand beinhaltet das gewählte Mittel?

Bei algorithmischen Systemen, die in Bewerbungsprozessen eingesetzt werden, geht es nicht um die finale Entscheidung, wer eingestellt werden soll, sondern um eine Bewerberinnenvorauswahl. Gegenüber algorithmischen Systemen, die Vorschläge für die Stellenbesetzung liefern, könnte man argumentieren, dass das Hochladen eines Lebenslaufs und eines Anschreibens ein milderes Mittel gegenüber dem Hochladen von Bewerbungsvideos o. Ä. ist. Allerdings gibt man beim Lebenslauf und auch beim Anschreiben zunächst mehr personenbezogene Daten preis als bei einem algorithmischen System, das die Ergebnisse anhand von Fragen wie z. B. „Warst du heute glücklich?“ generiert. Zwar stellt sich hier die Frage, welche Informationen das System aus den Antworten zieht. Wird aber verhindert, dass verfälschte Informationen[369] hervorgerufen werden, können mit einem algorithmischen System gezielter die gesuchten Informationen herausgefiltert werden als bei einem Lebenslauf, bei dem man ungefiltert eine große Menge personenbezogener Daten preisgibt. Allerdings kann bei einer automatisierten Datenverarbeitung ggf. auch stärker das allgemeine Persönlichkeitsrecht beeinträchtigt werden als bei einem Gespräch mit einem Menschen: Letzterer nimmt Aspekte häufig nur flüchtig wahr, wohingegen ein algorithmisches System personenbezogene Daten sehr detailliert verarbeiten kann.[370]

Auch findet ein herkömmliches Bewerbungsinterview in der Regel mit der Arbeitgeberin oder während eines Assessment-Centers mit einer Wirtschaftspsychologin statt.[371] Ein solches Verfahren ist gegenüber einem algorithmischen Verfahren zum einen zeitintensiver: Neben der Anfahrt muss die Bewerberin i. d. R. einen halben bis ganzen Tag einplanen, um verschiedene Interviews zu absolvieren. Selbst wenn es sich nur um ein

---

[369] S. dazu vorheriges Beispiel Kapitel 6 C.IV.2.b)aa) (S. 176).

[370] *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 232 f.

[371] *Betz*, ZD 2019, 148, 149.

Interview handelt, ist der Einsatz eines algorithmischen Systems weniger zeitintensiv.[372] Zum anderen dürfte ein Gespräch mit einer unbekannten Person belastender sein als ein automatisiertes Interview oder das bloße Hochladen aufgenommener Videos auf einer Plattform.[373] Bei einem Gespräch mit einer realen Person hat man eine einzige Chance, einen guten Eindruck zu hinterlassen. Bei einem maschinell lernenden System hingegen, welches ein Video oder Stimmaufnahmen auf bestimmte Merkmale hin analysiert, hat man mehrere Versuche.[374] Man kann die Antwort erst abschicken, wenn man selbst zufrieden ist. Mithin ist es möglich, Aussagen zu korrigieren oder anzupassen. Diese Möglichkeit hat man bei einem klassischen Auswahlgespräch nicht.

Als milderes Mittel gegenüber der Datenverarbeitung mittels algorithmischer Systeme kommt in Betracht, eine Personalerin gezielt dafür einzustellen, dass sie etwa stichprobenartig die Arbeit einzelner Personen überprüft.[375] Sammelt allerdings ein algorithmisches System diese Ergebnisse, muss die Arbeitgeberin, die Personalerin oder eine ähnliche Person zunächst nichts davon erfahren. Das algorithmische System könnte je nach Einsatzzweck nur die Arbeitsproben auswerten und danach einen Vorschlag liefern. Liefert das algorithmische System nach den vorgegebenen Regeln das treffende Ergebnis, kann der Einsatz eines Systems sogar milder sein: Wird ein Mensch eingesetzt, kann es stets sein, dass ggf. Nachteile für Arbeitnehmerinnen entstehen, wenn die Person, die für die Auswertung verantwortlich ist, interne Informationen preisgibt. Zwar dürfen die mit der Datenverarbeitung befassten Personen personenbezogene Daten nicht unbefugt verarbeiten (§ 53 BDSG) und mithin auch nicht weitergeben. Allerdings besteht bei Menschen grundsätzlich eher das Risiko, dass über bestimmte Vorgänge „getratscht" wird, etwa indem der Fall ohne Namensnennung geschildert wird. Es besteht somit unter Umständen ein Risiko für die betroffene Person. Bei einem algorithmischen System bestünde diese Gefahr zunächst nicht im selben Maße.

---

[372] *Ders.*, ZD 2019, 148, 149.

[373] *Ders.*, ZD 2019, 148, 149.

[374] S. zu derartigen Erfahrungen mit Videointerviews: *Teubert*, in: Gourmelon (Hrsg.), Personalauswahl – ein Blick in die Zukunft, 2018, 69.

[375] Vgl. BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327-1332, 1331.

Im Ergebnis ist ein rein menschlicher Auswahlprozess somit nicht unbedingt das mildere Mittel.[376]

bb) Gleiche Eignung

Angenommen, die oben erwähnten Verfahren sind gegenüber dem Einsatz eines algorithmischen Systems milder, dann muss das Verfahren *gleich geeignet* sein. Ein Verfahren ist gleich geeignet, wenn es in gleichem Maße wie das andere Verfahren das Ziel fördert.

Fraglich ist, ob man die gleiche Eignung in qualitativer oder quantitativer Hinsicht misst. Geht es darum, dass das jeweilige Verfahren im Einzelfall qualitativ gleich geeignet ist, oder geht es darum, dass das Verfahren in quantitativer Hinsicht, also bezogen auf eine Vielzahl von Fällen, gleich geeignet ist? Im Hinblick darauf unterscheiden sich menschliche Entscheidungen von algorithmischen Entscheidungen deutlich. Liegt eine Vielzahl an Bewerberinnen- oder Arbeitnehmerinnendaten vor, können algorithmische Systeme diese Daten viel schneller als menschliche Entscheider auswerten.[377] Im Hinblick auf die Qualität der einzelnen Entscheidungen weisen sowohl menschliche als auch algorithmische Entscheidungen Vor- und Nachteile auf.[378]

Überzeugend ist es, sowohl die qualitative als auch die quantitative Ebene bei der Frage nach der gleichen Eignung zu berücksichtigen. Sollen geeignete Bewerberinnen ausgewählt werden, muss zum einen gewährleistet sein, dass die Entscheidungen qualitativ hochwertig sind, und zum anderen, dass das jeweilige Verfahren für die Menge an Bewerberinnendaten gleich geeignet sein. Bei einer großen Anzahl auszuwertender Daten wird das algorithmische System in quantitativer Hinsicht sogar typischerweise besser geeignet ist als die menschliche Entscheidungsstruktur. Auch in qualitativer Hinsicht ist es möglich und häufig auch sinnvoll, dass man mithilfe algorithmischer Entscheidungen das risikobehaftete subjektive Gefühl von Personalerinnen

---

[376] I. E. auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 234; *Malorny*, JuS 2022, 289, 294.

[377] Kapitel 3 B. (S. 35).

[378] Kapitel 3 (S. 33).

außer Acht lässt und die Entscheidung aufgrund nachprüfbarer Parameter zustande kommt.[379] Ein algorithmisches System kann somit unter Umständen gleich – wenn nicht sogar besser – geeignet sein.

d) Angemessenheit

Im Rahmen der Angemessenheit müssen das Interesse der Arbeitgeberin an der Datenverarbeitung und das Persönlichkeitsrecht der Beschäftigten zu einem angemessenen Ausgleich gebracht werden.[380] Der Eingriff in das allgemeine Persönlichkeitsrecht ist unangemessen, wenn die rechtfertigenden Gründe außer Verhältnis zur Schwere des Eingriffs stehen.[381] Die Datenverarbeitung darf die Arbeitnehmerin nicht übermäßig belasten und muss der Bedeutung des Informationsinteresses der Arbeitgeberin entsprechen.[382] Bei der Abwägung muss eine Vielzahl an Gesichtspunkten berücksichtigt werden, die nun erläutert werden.

aa) Relevante Abwägungsgesichtspunkte

(1) Allgemeine Abwägungsgesichtspunkte

Franzen schlägt vor, im Rahmen des § 26 Abs. 1 S. 1 BDSG grundsätzlich folgende Abwägungsgesichtspunkte auf Seiten der Arbeitnehmerin zu berücksichtigen:[383]

- Zweck des Eingriffs, Leistungskontrolle oder Schutz von (vermögenswerten) Rechten oder Interessen der Arbeitgeberin, der Arbeitnehmerinnen oder Dritter, präventiv oder repressiv;

---

[379] Vgl. dazu auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 235.

[380] *BT-Drs. 18/11325*, S. 97; Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 13.

[381] BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327-1332, 1330.

[382] BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327-1332, 1330; BAG, 29.6.2017 – 2 AZR 597/16, NZA 2017, 1179, 1183.

[383] *Franzen*, ZfA 2019, 18, 33 f.

- Art des Eingriffs, verdeckt oder offen;[384]
- Intensität des Eingriffs in die Lebenssphäre der Arbeitnehmerin, ob die Sozial-, Privat-, oder Intimsphäre betroffen ist;
- Anlass des Eingriffs, Vorliegen konkreter Anhaltspunkte oder Eingriff „ins Blaue" hinein;
- Umfang des Eingriffs, stichprobenartig oder längerdauernd;[385]
- Einhaltung von Verfahrensregeln, etwa Hinzuziehung von Betriebsrat, der betrieblichen Datenschutzbeauftragten und der betroffenen Arbeitnehmerin.

Auf Seiten der Arbeitgeberin sei das Interesse an der Kenntnis der entsprechenden Daten zu berücksichtigen.[386] Eine höhere Eingriffsintensität sei etwa gerechtfertigt, wenn die Arbeitgeberin die Daten zum Schutz erheblicher Vermögensinteressen verarbeite. Zuletzt seien die Stadien des Arbeitsverhältnisses (Begründung, Durchführung, Beendigung) bei der Bewertung zu berücksichtigen. Welche Rolle die Stadien des Arbeitsverhältnisses bei der Abwägung spielen, führt *Franzen* aber nicht näher aus. Vermutlich bezieht sich die Aussage aber auf unterschiedliche Interessen und Schutzwürdigkeit der Arbeitnehmerin und Arbeitgeberin je nach Stadium des Arbeitsverhältnisses. Im Bewerbungsprozess ist eine Bewerberin z. B. weniger schutzwürdig, wenn sie sich mit hoher Qualifikation auf viele Stellen bewirbt. Im bestehenden Arbeitsverhältnis ist die Arbeitnehmerin schon deshalb besonders schutzwürdig, weil das Arbeitsverhältnis bzw. die berufliche Tätigkeit der Schaffung und Erhaltung der Lebensgrundlage dient.[387]

Welche Abwägungskriterien im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO berücksichtigt werden müssen, ist gesetzlich nicht vorgegeben. Die genannten

---

[384] So auch *Niklas/Thurn*, BB 2017, 1589, 1592; s. dazu auch die Rechtsprechung des BAG zur Videoüberwachung: BAG, 31.1.2019 – 2 AZR 426/18, NZA 2019, 893; BAG, 28.3.2019 – 8 AZR 421/17, NZA 2019, 1212; s. dazu auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 237 f.; *Wedde*, Automatisierung im Personalmanagement – arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, 2020, S. 10 ff.

[385] BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327-1332.

[386] *Franzen*, ZfA 2019, 18, 34.

[387] Vgl. Jarass/Pieroth/*Jarass*, Art. 12 GG Rn. 6.

Abwägungskriterien zielen jedoch alle darauf ab, die Schwere des Eingriffs in das jeweilig betroffene Grundrecht zu bestimmen. Die genannten Kriterien sollten daher auch im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO berücksichtigt werden. Mithilfe einer Abwägung kann allerdings nicht gerechtfertigt werden, was gegen Grundprinzipien der DSGVO verstößt. So ist es nach der DSGVO nicht möglich, Daten geheim zu verarbeiten.[388]

(2) Öffentlich zugängliche Daten vs. Grundsatz der Direkterhebung

Auf Seiten der Arbeitgeberin kann man zudem berücksichtigen, um welche Art von Daten es sich handelt. Personenbezogene Daten, die Bewerberinnen öffentlich zugänglich gemacht haben, sind – so könnte man meinen – weniger schutzbedürftig.[389] Allerdings gab es, bevor die DSGVO und das BDSG n.F. in Kraft getreten sind, den sog. Grundsatz der Direkterhebung. Dieser war in § 4 Abs. 2 S. 1 BDSG a. F. normiert und beinhaltete, dass personenbezogene Daten beim Betroffenen selbst, also bei der Bewerberin oder bei der Arbeitnehmerin, zu erheben sind.[390] Obwohl dieser Grundsatz nicht im BDSG n. F. und auch nicht in der DSGVO enthalten ist, wird er teilweise weiterhin über den Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a DSGVO angewendet.[391] Die personenbezogenen Daten seien weiterhin bei der betroffenen Person direkt zu erheben.[392]

Der Grundsatz der Direkterhebung ist aber im Vergleich zum BDSG a. F. nicht mehr ausdrücklich normiert. Würde man den Grundsatz der Direkterhebung weiterhin als Grundlage für die Datenerhebung berücksichtigen, würde man nicht hinreichend den Willen des Verordnungsgebers berücksichtigen, der den Grundsatz der Direkterhebung nicht erwähnt hat.[393] Es ist daher überzeugend, dass der Grundsatz der

---

[388] *Wünschelbaum*, NZA 2023, 487, 545.

[389] *Hoffmann*, NZA 2022, 19, 23.

[390] *Däubler*, Gläserne Belegschaften, 9. Aufl., § 5 Rn. 202; s. dazu auch: *Neff*, DSRITB 2015, 81.

[391] *Bartsch/Oerke*, IR 2022, 155; *Gola*, NZA 2019, 654, 655; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 34 ff.

[392] *Däubler*, Gläserne Belegschaften, 9. Aufl., § 5 Rn. 203.

[393] *Thüsing*, in: Thüsing/Wurth (Hrsg.), Social Media im Betrieb, 2. Aufl. 2020, § 1 Rn. 10.

Direkterhebung nicht mehr entgegensteht, wenn Daten nicht unmittelbar bei der Betroffenen erhoben werden.

Insbesondere dürfen Daten erhoben werden, wenn es sich um öffentlich verfügbare Daten handelt, die die betroffene Person bewusst veröffentlicht: Die Daten sind auch noch öffentlich, wenn sie in einem sozialen Netzwerk verbreitet werden, das durch ein Passwort zugänglich ist.[394] Die Hürde der Anmeldung kann leicht überwunden werden. Wichtig ist aber, dass die Betroffenen mit der Veröffentlichung der Daten auch eine bewusste Außenwirkung erzielen möchten. Veröffentlichen sie bestimmte Informationen etwa nur für bestimmte Gruppen, ist zum einen die Zugangsschranke höher und zum anderen gibt die Person damit zu erkennen, dass diese Informationen nicht für die Öffentlichkeit bestimmt sind. In solchen Fällen wird die Angemessenheitsprüfung eher zulasten der Arbeitgeberin und somit gegen die Verarbeitung der Daten ausfallen.[395] *LinkedIn* hingegen ist ein Beispiel dafür, dass eine bewusste Außenwirkung erzielt werden soll; die Verarbeitung derartiger Daten greift weniger schwer in das Persönlichkeitsrecht des Betroffenen ein.[396]

Auch wenn der Grundsatz der Direkterhebung nicht mehr zu berücksichtigen ist, kann die Datenerhebung unmittelbar bei der betroffenen Person ggf. aus anderen Gründen nicht gerechtfertigt sein, etwa weil sie nicht erforderlich i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO ist.[397]

(3) Interesse an objektiver Auswahlentscheidung und Bewältigung großer Datenmengen

Auf Seiten der Arbeitgeberin muss zudem berücksichtigt werden, mit welchem Ziel sie das algorithmische System einsetzt. Die Arbeitgeberin setzt das algorithmische System mit dem Ziel ein, eine objektive Auswahlentscheidung, wie es bei einer rein menschlichen

---

[394] *Dallmann/Busse*, ZD 2019, 394, 396; *Gola*, NZA 2019, 654, 656.

[395] Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 36.

[396] *Byers/Fischer*, ArbRAktuell 2022, 90, 92; *Dallmann/Busse*, ZD 2019, 394, 396; differenziert dazu auch: *Däubler*, Gläserne Belegschaften, 9. Aufl., § 5 Rn. 247 ff.

[397] Vgl. *Thüsing*, in: Thüsing/Wurth (Hrsg.), Social Media im Betrieb, 2. Aufl. 2020, § 1 Rn. 11.

Auswahlentscheidung kaum möglich wäre, zu treffen. Angenommen, das algorithmische System ist insgesamt geeignet[398], dieses Ziel zu erreichen, und im Übrigen auch erforderlich[399], so wird der Datenverarbeitung mittels des Systems angemessen sein, solange keine überwiegenden Interessen der Arbeitnehmerin entgegenstehen. Auf jeden Fall muss die konkrete Situation der Arbeitgeberin berücksichtigt werden. Der Einsatz eines algorithmischen Systems und die entsprechende Datenverarbeitung sind eher angemessen, wenn die Arbeitgeberin ansonsten die Datenmengen nicht sichten kann. Wird eine Vielzahl an Bewerbungen eingereicht, die die Arbeitgeberin ohne Zuhilfenahme eines algorithmischen Systems nicht auswerten kann, spricht das auch eher dafür, dass es angemessen ist, ein solches System einzusetzen.

(4) Kein Erstellen eines umfassenden Persönlichkeitsprofils

Die Interessen der Arbeitnehmerin überwiegen, wenn zu intensiv in ihr Persönlichkeitsrecht eingegriffen wird, etwa indem durch ein eingesetztes Mittel ein „umfassendes und lückenloses" Profil über die betroffene Arbeitnehmerin erstellt wird.[400] Mithin war der Einsatz eines *Keyloggers*, mit dessen Hilfe ein solches Profil erstellt werden konnte, in dem vom BAG entschiedenen Fall nicht angemessen.[401] Zu einem ähnlichen Ergebnis ist das BAG in seinem Urteil zu einer Belastungsstatistik[402] gekommen, anhand der die Arbeitgeberin die Belastungssituation der Arbeitnehmerinne erfassen wollte, um die Arbeitsabläufe umzugestalten und zu verbessern.[403] Die nahezu lückenlose Erfassung einzelner Arbeitsschritte war nicht durch überwiegend schutzwürdige Belange der Arbeitgeberin gedeckt, sodass der schwerwiegende dauerhafte Eingriff in das Persönlichkeitsrecht der Arbeitnehmerinnen im

---

[398] S. dazu: Kapitel 6 C.IV.2.b) (S. 176).

[399] Kapitel 6 C.IV.2.c) (S. 176).

[400] BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327-1332, 1331 Rn. 33; *Däubler*, Gläserne Belegschaften, 9. Aufl., § 7 Rn. 429 b; *Grimm/Singraven*, Digitalisierung und Arbeitsrecht, 2022, § 16 Rz. 16.10.

[401] BAG, 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327, 1330; s. dazu bereits: Kapitel 6 C.IV.2.a) (S. 175).

[402] BAG, 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205.

[403] BAG, 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205, 1212.

Ergebnis unangemessen war.[404] Die Arbeitnehmerinnen dürfen somit nicht permanent anlasslos „überwacht" werden.

(5) Grenze: Fragerecht der Arbeitgeberin

Möglich ist es aber, innerhalb der Grenzen des Fragerechts der Arbeitgeberin[405] zulässige Auswertungen mithilfe algorithmischer Systeme zu erstellen. Dabei ist im konkreten Fall zu prüfen, ob ein Merkmal, welches etwa das algorithmische Systeme herausfiltert, für den konkreten Fall relevant ist. Nicht gefragt werden darf etwa nach Lebensverhältnissen der Bewerberin, die in keinem notwendigen Zusammenhang mit dem Arbeitsverhältnis stehen.[406] Die Arbeitgeberin darf die Bewerberin aber nach fachlichen und persönlichen Fähigkeiten und Erfahrungen fragen.[407] Grundsätzlich steht der Arbeitnehmerin bei unzulässigen Fragen ein „Recht zur Lüge" zu.[408] Beispielsweise darf man die Frage nach der Schwangerschaft unrichtig beantworten. Aufgrund seines Geschlechts darf man nicht diskriminiert werden.[409] Unzulässig ist es deshalb, ein umfassendes Persönlichkeitsprofil mithilfe algorithmischer Systeme einer Person zu erstellen.[410] Ein solches umfassendes Persönlichkeitsprofil beschränkt sich nicht auf die Fragen, die für das konkrete Arbeitsverhältnis relevant sind, sondern enthält auch Informationen, die ohne Bezug zum Arbeitsverhältnis stehen.

---

[404] BAG, 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205, 1212.

[405] Dazu bereits unter: Kapitel 6 C.IV.2.b)bb); *Götz*, Big Data im Personalmanagement, 2020, S. 96; *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 243 ff.

[406] S. zur Zulässigkeit einzelner Fragen: *Däubler*, Gläserne Belegschaften, 9. Aufl., § 5 Rn. 210 ff.

[407] *Ders.*, Gläserne Belegschaften, 9. Aufl. 2021, § 5 Rn. 221.

[408] *Ders.*, Gläserne Belegschaften, 9. Aufl. 2021, § 5 Rn. 225.

[409] *Ders.*, Gläserne Belegschaften, 9. Aufl. 2021, § 5 Rn. 215.

[410] ErfK/*Franzen*, § 26 BDSG Rn. 13; Kühling/Buchner/*Maschmann*, § 26 BDSG Rn. 33; Gola/Heckmann/*Pötters*, § 26 BDSG Rn. 166; *Niklas/Hoffmann*, ArbRB 2021, 283, 285; *Block*, 23. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 52 f.; *Betz*, ZD 2019, 148, 150; *Dzida*, NZA 2017, 541, 545.

(6) Nähe zur Menschenwürde gem. Art. 1 GRCh: Wahrung personaler Individualität

Das Fragerecht der Arbeitgeberin droht aber bei algorithmischen Systemen teilweise entwertet zu werden [411]: Werten algorithmische Systeme das Verhalten oder Merkmale von Menschen aus, um herauszufinden, ob die Person Kompetenzen wie z. B. Teamfähigkeit oder Empathiefähigkeit hat, besteht ein Bezug zum konkreten Arbeitsverhältnis. Man kann daher argumentieren, dass man nach diesen Kriterien bewertet werden muss. Allerdings könnte dieses Vorgehen dazu führen, dass ein (umfassendes) Persönlichkeitsprofil der Person erstellt wird. Deshalb muss noch ein zusätzlicher Maßstab hinzukommen: Es muss berücksichtigt werden, dass die „personale Individualität" [412] gewahrt wird. Das garantiert die Menschenwürde nach Art. 1 Abs. 1 GG, die „insbesondere die Wahrung personaler Individualität, Identität und Integrität" [413] umfasst. Dem Menschen wird eine Subjektqualität zugeschrieben, der ein sozialer Wert- und Achtungsanspruch zuteilwird. [414] Demnach darf der Mensch nicht zum „bloßen Objekt" staatlichen Handelns degradiert werden. [415] Im Privatrechtsverhältnis entfaltet Art. 1 Abs. 1 GG unmittelbare Drittwirkung.[416] Im Unionsrecht ist die Würde des Menschen in Art. 1 GRCh verankert. Wie auch Art. 1 Abs. 1 GG ist mit der Menschenwürde, die durch Art. 1 GRCh garantiert ist, der soziale Wert- und Achtungsanspruch gemeint, der dem Menschen zukommt.[417] Wie auch Art. 1 Abs. 1 GG entfaltet Art. 1 GRCh richtigerweise unmittelbare Drittwirkung im Privatrechtsverhältnis.[418]

---

[411] *Götz*, Big Data im Personalmanagement, 2020, S. 101; vgl. *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 246 f.

[412] BVerfG, 17.1.2017 – 2 BvB 1/13, NJW 2017, 611, 619.

[413] BVerfG, 17.1.2017 – 2 BvB 1/13, NJW 2017, 611, 619.

[414] Vgl. auch *Nink*, Justiz und Algorithmen, 2021, S. 350 f.

[415] BVerfG, 17.1.2017 – 2 BvB 1/13, NJW 2017, 611, 619.

[416] BVerfG, 17.1.2017 – 2 BvB 1/13, NJW 2017, 611, 619; Dürig/Herzog/Scholz/*Herdegen*, Art. 1 Abs. 1 GG Rn. 74.

[417] Jarass/Pieroth/*Jarass*, Art. 1 GRCh Rn. 6 m. w. N.; a. A.: Calliess/Ruffert/*Calliess*, Art. 1 GRCh Rn. 7.

[418] NK-GRC/*Borowsky*, Art. 1 GRCh Rn. 43.

Werden mithilfe von maschinell lernenden Systemen Verhaltensweisen von Menschen analysiert und darauf aufbauend Vorhersagen über bestimmte Eigenschaften, zukünftige Erfolgschancen im Beruf oder mögliche Kündigungsabsichten getroffen, wird menschliches Verhalten „berechenbar" gemacht.[419] Mithilfe großer Datensätze deckt das maschinell lernende System Korrelationen auf, die zu neuen Erkenntnissen führen. Auf Basis der Ergebnisse werden Menschen in Kategorien eingeordnet und kommen je nach Ergebnis für eine Position in Betracht oder nicht. Menschliche Verhaltensweisen werden nicht als etwas Unergründliches und Individuelles wahrgenommen, sondern gelten als berechenbar und mithin vergleichbar.[420] Die Akzeptanz des Individuums mit unzähligen Persönlichkeitsfacetten gerät in den Hintergrund.[421] Eine solche „Katalogisierung" der individuellen Persönlichkeit ist nicht mit der Menschenwürde vereinbar.[422] In solchen Fällen findet keine Abwägung mehr statt, weil die Menschenwürde absolut geschützt ist.[423] Diese Erwägungen müssen richtigerweise auch im Rahmen von Art. 1 GRCh berücksichtigt werden.

bb) Angemessenheit des Einsatzes algorithmischer Systeme

Die Angemessenheit algorithmischer Systeme ist nach den dargelegten Abwägungsfaktoren zu beurteilen.

Werden im Bewerbungsverfahren algorithmische Systeme eingesetzt, steht dem der Grundsatz der Direkterhebung nicht entgegen, wenn Daten nicht unmittelbar bei der Betroffenen erhoben werden. Öffentlich verfügbare Daten dürfen vor allem dann verarbeitet werden, wenn die betroffene Person diese bewusst veröffentlicht hat. Die Datenerhebung, die nicht unmittelbar bei der betroffenen Person erfolgt, kann aber aus anderen Gründen nicht

---

[419] S. dazu auch: *Cheng/Hackett*, Human Resource Management Review 31 (2021), 1, 5 f.

[420] *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 247.

[421] *Dreyer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, 139.

[422] *Gola*, RDV 2018, 24, 27; *Wedde*, Automatisierung im Personalmanagement – arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, 2020, S. 42, der ein klares gesetzliches Verbot für solche Systeme fordert.

[423] BVerfG, 9.12.2022 – 1 BvR 1345/21, juris, Rn. 102; Dürig/Herzog/Scholz/*Herdegen*, Art. 1 Abs. 1 GG.

rechtmäßig sein, etwa weil sie nicht erforderlich i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO ist. Es ist daher – auch bei öffentlich verfügbaren Daten – im Einzelfall zu prüfen, ob die Verarbeitung dieser Daten erforderlich ist.[424] Die Intention, mit welcher die betroffene Person die Daten verarbeitet hat, muss aber hinreichend berücksichtigt werden und kann ggf. den Ausschlag geben, dass diese Daten eher verarbeitet werden können. Auf Seiten der Arbeitgeberin ist insbesondere zu berücksichtigen, für welche Zwecke und in welchem Kontext sie das algorithmische System einsetzt. Die Datenverarbeitung mittels algorithmischer Systeme ist eher angemessen, wenn die Arbeitgeberin eine objektive Auswahlentscheidung herbeiführen will oder ansonsten der Menge der Daten nicht gerecht wird.

Werden algorithmische Systeme im Bewerbungskontext eingesetzt, um die Bewerberinnen auf bestimmte Merkmale hin zu analysieren, ist das nur in engen Grenzen möglich. Es darf kein umfassendes Persönlichkeitsprofil von den Kandidatinnen erstellt werden. Sprachanalysen oder Videoanalysen, die solche Profile erstellen, sind daher unangemessen und insgesamt nicht erforderlich i. S. d. § 26 Abs. 1 S. 1 BDSG.[425] In solchen Fällen liegt ein unverhältnismäßiger Eingriff in das allgemeine Persönlichkeitsrecht nach Art. 1 Abs. 1 GG i. V. m. 2 Abs. 1 GG vor, bei dem es keine Interessen der Arbeitgeberinnen gibt, die den Eingriff rechtfertigen. Vielmehr dürfen solche Systeme in den Grenzen des Fragerechts der Arbeitgeberin Auswertungen vornehmen, die für die konkrete Stelle relevant sind. Etwa kann man die Qualifikation der Kandidatin auf der Grundlage bestimmter Kriterien wie z. B. Berufserfahrung oder Expertise überprüfen. Zudem muss die Nähe zur Menschenwürde berücksichtigt werden: Dem Einzelnen darf nicht seine Individualität abgesprochen werden, indem Eigenschaften oder Verhaltensweisen vom System „berechnet“ werden. Derartige Systeme sind

---

[424] S. *Dallmann/Busse*, ZD 2019, 394.

[425] *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 254; *Gola*, RDV 2018, 24, 27; Hoeren/Sieber/Holznagel, MultimediaR-Hdb/*John*, Teil 29.4 KI im Arbeitsrecht Rn. 24 ff.; a. A. *Jares/Vogt*, in: Knappertsbusch/Gondlach (Hrsg.), Arbeitswelt und KI 2030, 2021, 78.

daher wegen des Verstoßes gegen die Menschenwürde gem. Art. 1 Abs. 1 GG unangemessen.[426]

Bei algorithmischen Systemen, die im bestehenden Arbeitsverhältnis eingesetzt werden, darf die Arbeitnehmerin nicht einem permanenten Überwachungsdruck ausgesetzt sein. Algorithmische Systeme, die die Leistung der Arbeitnehmerinnen ständig messen, sind daher unzulässig. Es ist aber möglich, stichprobenartig die Arbeit der Arbeitnehmerinnen zu überprüfen.

3. Zwischenergebnis zur Erforderlichkeit

1. Im Ergebnis kann es somit je nach Einzelfall erforderlich sein, ein algorithmisches System zur Verarbeitung personenbezogener Daten im Beschäftigungskontext einzusetzen. Dabei muss ein maschinell lernendes System auf Ebene der Geeignetheit insbesondere eine hohe Qualität der Trainingsdaten aufweisen, damit sachfremde Erwägungen nicht mit in das Ergebnis einfließen.[427] Zudem darf das algorithmische System nur zulässige Fragen in Bezug auf die konkrete Tätigkeit stellen.[428] Es darf die Person mithin auch nicht auf Merkmale hin analysieren, die für die relevante Tätigkeit nicht von Belang sind.

2. Auf Ebene der Erforderlichkeit darf es kein milderes, gleich geeignetes Mittel geben.[429] Je nach Anwendungsfall kann ein algorithmisches System gegenüber herkömmlichen Verfahren zur Bewerberinnenvorauswahl oder Auswahl von Arbeitnehmerinnen, die z. B. befördert werden sollen, sogar milder sein. Das ist der Fall, wenn bei einem algorithmischen System der Vorgang wiederholt und mithin „geübt“ werden kann. Das ist bei einem tatsächlichen Gespräch nicht möglich – es gibt nur einen ersten Eindruck.

---

[426] S. dazu auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 251 f.

[427] Kapitel 6 C.IV.2.b)aa) (S. 176).

[428] Kapitel 6 C.IV.2.b)bb) (S. 177).

[429] Kapitel 6 C.IV.2.c) (S. 178).

3. Sofern ein milderes Mittel vorliegt, muss dieses auch gleich geeignet sein.[430] Die gleiche Eignung ist sowohl in quantitativer als auch in qualitativer Hinsicht zu beurteilen. Je nach Anwendungsfall können algorithmische Systeme sogar besser geeignet sein als herkömmliche Verfahren: Wenn eine Vielzahl an Daten ausgewertet werden soll, ist dies für eine menschliche Person nicht ohne Weiteres möglich.

4. Zuletzt muss der Einsatz eines algorithmischen Systems auch angemessen sein.[431] Dabei ist das Interesse der Arbeitgeberin an der Datenverarbeitung und das Persönlichkeitsrecht der betroffenen Person gegeneinander abzuwägen. Bei der Angemessenheitsprüfung müssen verschiedene Abwägungskriterien berücksichtigt werden. Zu berücksichtigen ist insbesondere, dass Arbeitnehmerinnen nicht permanent überwacht werden dürfen, eine umfassende Persönlichkeitsprofilerstellung unzulässig ist und der Person nicht ihre Individualität abgesprochen werden darf.[432]

V. Betriebsvereinbarungen

Nach Art. 88 Abs. 1 DSGVO können die Mitgliedstaaten auch durch Kollektivvereinbarungen spezifischere Vorschriften hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext treffen. Unter dem Begriff „Kollektivvereinbarungen“ sind nach Erwägungsgrund 155 DSGVO ausdrücklich auch Betriebsvereinbarungen erfasst.

Der Wortlaut der Norm verwundert, denn Mitgliedsstaaten können nur durch Gesetze bereichsspezifische Vorschriften erlassen, aber keine Kollektivvereinbarungen schließen. Kollektivvereinbarungen i. S. d. Art. 88 Abs. 1 DSGVO können nur Tarifvertragsparteien oder Betriebsparteien treffen, die der Wortlaut des Art. 88 Abs. 1 DSGVO nicht erwähnt. Die Norm erfüllt ihren Regelungszweck aber nur, wenn sie so verstanden wird, dass Art. 88 Abs. 1 DSGVO Tarifvertragsparteien und Betriebsparteien mit der Befugnis ausstattet, Vereinbarungen zum Zwecke der Datenverarbeitung im

[430] Kapitel 6 C.IV.2.c)bb) (S. 181).
[431] Kapitel 6 C.IV.2.d) (S. 182).
[432] Kapitel 6 C.IV.2.d)aa)(6) (S. 188).

Beschäftigungskontext zu treffen.[433] Da Staaten – wie erwähnt – keine arbeitsrechtlichen Kollektivvereinbarungen schließen können, wäre die Nennung solcher Vereinbarungen in Art. 88 Abs. 1 DSGVO sonst ohne Bedeutung.

Die diskutierten Probleme rund um Art. 88 DSGVO sind komplex und werden im folgenden Abschnitt nur behandelt, soweit sie den Untersuchungsgegenstand dieser Arbeit betreffen.[434] Wichtig für den Untersuchungsgegenstand ist, ob Betriebsvereinbarungen als Rechtsgrundlage für eine Datenverarbeitung dienen können.[435] Außerdem wird herausgearbeitet, ob durch Betriebsvereinbarungen i. S. d. Art. 88 Abs. 1 DSGVO vom Schutzstandard der DSGVO abgewichen werden darf.[436]

1. Betriebsvereinbarung als Rechtsgrundlage für die Datenverarbeitung

Der Begriff „Kollektivvereinbarungen" in Art. 88 Abs. 1 DSGVO ist als unbestimmter unionsrechtlicher Rechtsbegriff zwar autonom auszulegen.[437] In Erwägungsgrund 155 DSGVO wird jedoch – wie bereits erwähnt – ausdrücklich auf den Begriff der Betriebsvereinbarung Bezug genommen, sodass die deutsche Rechtsanwenderin davon ausgehen kann, dass Betriebsvereinbarungen i. S. d. BetrVG Kollektivvereinbarungen i. S. d. DSGVO sind. § 26 Abs. 4 S. 1 BDSG kann man entnehmen, dass Verarbeitungen personenbezogener Daten auf der Grundlage von Kollektivvereinbarungen zulässig sind.[438] Obwohl § 26 Abs. 4 BDSG vor allem klarstellende Bedeutung hat,[439] kann man die Vorschrift als systematisches

---

[433] Vgl. *Pötters*, Beschäftigtendatenschutz, 3. Aufl. 2021, Art. 88 DSGVO Rn. 13; *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 26 f.

[434] Ausführlich zu Art. 88 DSGVO: *Morasch*, Datenverarbeitung im Beschäftigungskontext, 2018; *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022.

[435] NK-Datenschutzrecht/*Seifert*, Art. 88 DSGVO Rn. 54; Forgó/Helfrich/Schneider/*Selk*, Kap. 3 C. II. 4. Rn. 90 f.; dazu sogleich unter: Kapitel 6 C.V.1. (S. 193).

[436] Kapitel 6 C.V.2. (S. 195).

[437] *Plote*, Arbeitsrecht im Zeitalter der Digitalisierung, S. 93, 101.

[438] *BT-Drs. 18/11325*, S. 98; so auch: *Dzida*, BB 2019, 3060, 3064; *Stück*, ZD 2019, 256; vgl. *Blum*, People Analytics, 2021, S. 120; *Flink*, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, 2020, S. 52; *Götz*, Big Data im Personalmanagement, 2020, S. 179.

[439] *BT-Drs. 18/11325*, S. 98; Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 46.

Argument dafür heranziehen, dass eine Betriebsvereinbarung als Rechtsgrundlage eingeordnet wird. Der deutsche Gesetzgeber hat den Unionsgesetzgeber dahingehend verstanden, dass eine Betriebsvereinbarung ein Erlaubnistatbestand sein kann.

Manche Autorinnen sind demgegenüber der Ansicht, dass „spezifischere Vorschriften", wie sie Art. 88 Abs. 1 DSGVO erlauben würden, nicht umfassen würden, eigene Erlaubnistatbestände zu schaffen.[440] Andere als die in Art. 6 DSGVO aufgeführten Erlaubnistatbestände seien in der DSGVO nicht vorgesehen. Deshalb seien Datenverarbeitungen stets am Erlaubnistatbestand des Art. 6 Abs. 1 DSGVO zu messen.[441]

Das überzeugt nicht. Der Gesetzgeber hat mit Art. 88 DSGVO eine Öffnungsklausel für den Beschäftigtendatenschutz geschaffen, die ein eigenständiger Erlaubnistatbestand ist.[442] Zwar spricht der Wortlaut nicht eindeutig von „Rechtsgrundlage" oder „Erlaubnistatbestand". Systematisch spricht für eine Einordnung als eigenständige Erlaubnisnorm aber Art. 88 Abs. 2 DSGVO, der weitere Vorgaben für die spezifischeren Vorschriften nach Art. 88 Abs. 1 DSGVO aufstellt. Art. 88 Abs. 2 DSGVO wäre überflüssig, würden Betriebsvereinbarungen an Art. 6 DSGVO gemessen werden.[443] Der Zweck des Art. 88 Abs. 1 DSGVO kann zudem nur darin bestehen, eine weitere Rechtsgrundlage in Form einer Betriebsvereinbarung für zulässig zu erklären.[444] Anderenfalls hätte der Verordnungsgeber nicht eine eigene Norm geschaffen, die eine Verarbeitung aufgrund einer Rechtsvorschrift oder Kollektivvereinbarung zulässt.[445]

---

[440] Forgó/Helfrich/Schneider/*Hanloser*, Teil V. Kap. 1 D. II. Rn. 51; Forgó/Helfrich/Schneider/*Selk*, Teil V. Kap. 3 C. II. 4. Rn. 106; *Monreal*, ZD 2022, 359.

[441] Forgó/Helfrich/Schneider/*Selk*, Teil V. Kap. 3 C. II. 4. Rn. 98.

[442] *Klösel/Mahnhold*, NZA 2017, 1428, 1429; *Köllmann*, Implementierung elektronischer Überwachungseinrichtungen durch Betriebsvereinbarung vor dem Hintergrund der DSGVO, 2021, S. 306 f.; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2015, S. 134; *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 101.

[443] *Klösel/Mahnhold*, NZA 2017, 1428, 1429.

[444] Vgl. NK-Datenschutzrecht/*Seifert*, Art. 88 DSGVO Rn. 26.

[445] *Klösel/Mahnhold*, NZA 2017, 1428, 1429.

Betriebsvereinbarungen können somit eine Verarbeitungsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext sein.

2. Abweichungen vom Schutzstandard der DSGVO möglich?

Was unter „spezifischeren Vorschriften" in Art. 88 Abs. 1 DSGVO gefasst wird, hat der unionsrechtliche Gesetzgeber nicht näher ausgeführt. Die Reichweite des Art. 88 Abs. 1 DSGVO ist nicht eindeutig und in Rechtsprechung und Schrifttum umstritten: Einerseits wird vertreten, eine Vorschrift sei nur spezifischer i. S. d. Art. 88 Abs. 1 DSGVO, wenn der vorgegebenen Rahmen der DSGVO gewahrt bleibe; die DSGVO sei vollharmonisierend.[446] Andere sind der Ansicht, dass Art. 88 Abs. 1 DSGVO eine Öffnungsklausel enthalte, die den Mitgliedstaaten erlaube, weitgehend autonom den Beschäftigtendatenschutz zu regeln.[447] Eine dritte Ansicht verfolgt den Ansatz der Mindestharmonisierung: Es seien nur Regelungen zulässig, die den Schutzgehalt der DSGVO beibehalten oder intensivieren würden.[448]

---

[446] BAG, 8 AZR 209/21 (A), NZA 2023, 363; LAG Berlin-Brandenburg, 4.6.2020 – 10 Sa 2130/19, NZA-RR 2020, 457, 458, das der Auffassung ist, Art. 88 DSGVO erlaube nur eine Konkretisierung oder Präzisierung, nicht jedoch eine Bereichsausnahme; so auch: *Monreal*, ZD 2022, 359, 363, der den Begriff Spezifizierungsklausel statt Öffnungsklausel für richtig erachtet; *Köllmann*, Implementierung elektronischer Überwachungseinrichtungen durch Betriebsvereinbarung vor dem Hintergrund der DSGVO, 2021, S. 223 ff.; *Morasch*, Datenverarbeitung im Beschäftigungskontext, 2018, S. 162 f.; Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 72 ff.; EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 10; Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rn. 25; *Holthausen*, RdA 2021, 19, 27; *Maschmann*, DB 2016, 2480, 2482.

[447] LAG Sachsen-Anhalt m. Anmerkung Wybitul/Böhm, 18.12.2018 – 4 TaBV 19/17, NZA-RR 2019, 256, 259, das in Art. 88 DSGVO eine Öffnungsklausel sieht; in die Richtung auch: *Körner*, NZA 2021, 1137, 1143; *Blum*, People Analytics, 2021, S. 121 ff.; *Flink*, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, 2020, S. 194 ff.; *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 44 ff.; BeckOK Datenschutzrecht/*Riesenhuber*, Art. 88 DSGVO Rn. 69.

[448] *Kersting*, in: Buhl/Frieling/Krois u.a. (Hrsg.), Der erwachte Gesetzgeber, 2017, S. 55, 73; *Körner*, NZA 2016, 1383; *Wurzberger*, ZD 2017, 258, 263.

Im Kern dreht sich die Beantwortung der Frage darum, ob durch Art. 88 DSGVO eine Mindest- oder Vollharmonisierung im Beschäftigungskontext erzielt werden soll.[449]

a) Unterschiedliche Auffassungen in Literatur und Rechtsprechung

aa) Keine Abweichung vom Schutzstandard der DSGVO möglich

Viele halten eine Absenkung des Datenschutzniveaus nicht für möglich.[450] Für Art. 88 DSGVO gelte das Prinzip der Vollharmonisierung, weshalb das von der DSGVO vorgegebene Niveau für den Beschäftigtendatenschutz verbindlich sei. [451] Bereits für die DSRL habe das Prinzip der Vollharmonisierung gegolten. [452] Die DSRL habe den freien Verkehr personenbezogener Daten sicherstellen wollen und gleichzeitig ein hohes Niveau des Schutzes der Rechte und Interessen der betroffenen Personen gewährleisten wollen. [453] Diese Erwägungen müssten auch auf die DSGVO übertragen werden.[454] Hinzu komme auch die Rechtsnatur der DSGVO als Verordnung: Mehr noch als die vorherige Richtlinie müsse sie aufgrund ihrer Rechtsnatur eine Vollharmonisierung bewirken. [455] Ließe man abweichende Regelungen zu, führte das zu einer Zersplitterung des Datenschutzniveaus, da

---

[449] *Maschmann*, DB 2016, 2480, 2482; *Morasch*, Datenverarbeitung im Beschäftigungskontext, 2018, S. 62.

[450] BAG, 8 AZR 209/21 (A), NZA 2023, 363; Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 92; Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rn. 23, der keine wesentlichen Abweichungen für möglich hält; Kühling/Buchner/*Maschmann*, Art. 88 DSGVO Rn. 40; Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 4; *Körner*, NZA 2019, 1389, 1395; *Maschmann*, DB 2016, 2480, 2484; *Stück*, ZD 2019, 256, 257;

[451] EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 10; Kühling/Buchner/*Maschmann*, Art. 88 DSGVO Rn. 40; *Dzida/Grau*, DB 2018, 189, 193; *Franzen*, EuZA 2017, 313, 345.

[452] EuGH, 6.11.2003 – C-101/01, EuZW 2004, 245, 252; *Plote*, Arbeitsrecht im Zeitalter der Digitalisierung, S. 93, 102.

[453] EuGH, 6.11.2003 – C-101/01, EuZW 2004, 245, 252.

[454] Vgl. EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 10; Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rn. 24; Kühling/Buchner/*Maschmann*, Art. 88 DSGVO Rn. 30.

[455] Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rn. 24.

gerade keine einheitlichen Vorschriften in den Mitgliedstaaten gelten würden.[456]

Häufig wird auch auf die Entscheidung des EuGH vom 24. November 2011[457] zur Auslegung der DSRL (*ASNEF*-Entscheidung) verwiesen. In diesem Urteil hat der EuGH untersucht, ob Art. 7 DSRL, der den Erlaubnisvorbehalt der Datenverarbeitung sowie sechs Erlaubnistatbestände regelte, abschließend gelte oder für mitgliedstaatliche Gestaltungen offen sei. Er stellte fest, dass Art. 7 DSRL eine erschöpfende und abschließende Liste für die rechtmäßige Datenverarbeitung vorsehe. Der spanische Gesetzgeber habe den mitgliedsstaatlichen Gestaltungsspielraum dadurch überschritten, indem er die einwilligungslose Datenverarbeitung ausschließlich für öffentlich zugängliche Daten vorgesehen hätte. Viele sehen die Entscheidung auch als maßgeblich für die DSGVO an: Auch hier gelte das Prinzip der Vollharmonisierung.[458] Die Vorgaben der DSGVO müssten daher eingehalten werden.

bb) Abweichungen „nach unten" nur im Ausnahmefall möglich

Abweichungen „nach unten" und damit einhergehend Verschlechterungen des Datenschutzniveaus durch Kollektivvereinbarungen sind nach der überwiegenden Ansicht nicht möglich.[459] Das sei vor allem auf den Wortlaut von Art. 88 Abs. 1 und 2 DSGVO zurückzuführen, die den Schutz personenbezogener Daten als Ziel der nationalen Vorschriften und Kollektivvereinbarungen nennen.[460] Dieser Schutz personenbezogener Daten dürfe nicht durch abweichende Regelungen verschlechtert werden. *Pötters* ist

---

[456] Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 76.

[457] EuGH, 24.11.2011 – C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito ASNEF [C-468/10]; Federación de Comercio Electrónico y Marketing Directo FECEMD [C-469/10] ./. Administración del Estado*, NZA 2011, 1409.

[458] Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 16; Kühling/Buchner/*Maschmann*, Art. 88 DSGVO Rn. 30; *Franzen*, EuZA 2017, 313, 345 Fn. 87; *Monreal*, ZD 2022, 359, 360 Fn. 30.

[459] Statt vieler: Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rn. 26; Sydow/Marsch/*Tiedemann*, Art. 88 DSGVO Rn. 3; Taeger/Gabel/*Zöll*, Art. 88 DSGVO Rn. 17; *Morasch*, Datenverarbeitung im Beschäftigungskontext, 2018, S. 61 m. w. N.

[460] Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rn. 26.

der Ansicht, dass „gewisse Sonderwege im Hinblick auf formelle Aspekte“ möglich sein müssten.[461] Er führt das aber nicht näher aus. Jedenfalls dürfe man nicht vom materiellen Schutzstandard der Art. 6-9 sowie des Art. 5 und der Art. 12 ff. DSGVO abweichen. Die Ansicht von *Pötters* schließt eine Abweichung „nach unten“ indes nicht aus.

Riesenhuber sieht das ähnlich und hält eine Absenkung des Schutzniveaus durch spezifischere Vorschriften i. S. d. Art. 88 DSGVO nicht für ausgeschlossen. Spezifischere Vorschriften würden andersartige Schutzmechanismen umfassen, ob diese „stärker“ oder „schwächer“ seien, sei nicht zwingend vorgegeben.[462]

cc) Abweichung „nach oben“ möglich

Andere Stimmen in der Literatur sind der Ansicht, dass die DSGVO lediglich ein Mindestschutzniveau vorschreibe, sodass günstigere nationale Regelungen im Beschäftigungskontext geschafft werden könnten.[463]

Spezifischere Vorschriften gingen vor allem über die allgemeinen Regeln der DSGVO hinaus und würden somit von den Vorgaben der DSGVO zwangsläufig „nach oben“ abweichen.[464] § 26 Abs. 2 S. 3 BDSG fordere etwa gegenüber Art. 7 Abs. 2 DSGVO ein Schriftformerfordernis für die Einwilligung. Verbiete man generell datenschutzfreundlichere Vorschriften, würde die Bewegungsfreiheit der Mitgliedstaaten stark eingeengt und der Zweck von Art. 88 Abs. 1 DSGVO vereitelt werden.[465] Dieser liegt darin, dass den Mitgliedstaaten ein Gestaltungsspielraum im Beschäftigungskontext zukommt.[466]

---

[461] Gola/Heckmann/*ders.*, Art. 88 DSGVO Rn. 27.

[462] BeckOK Datenschutzrecht/*Riesenhuber*, Art. 88 DSGVO Rn. 67; so auch: *Flink*, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, 2020, S. 195; *Franzen*, NZA 2020, 1593, 1595.

[463] Sydow/Marsch/*Tiedemann*, Art. 88 DSGVO Rn. 3; NK-Datenschutzrecht/*Seifert*, Art. 88 DSGVO Rn. 23; *Körner*, NZA 2019, 1389, 1390; *Kort*, DB 2016, 711, 714.

[464] NK-Datenschutzrecht/*Seifert*, Art. 88 DSGVO Rn. 23.

[465] NK-Datenschutzrecht/*ders.*, Art. 88 DSGVO Rn. 23.

[466] Vgl. NK-Datenschutzrecht/*ders.*, Art. 88 DSGVO Rn. 23.

b) Prinzipielles Schutzniveau des Art. 88 Abs. 2 DSGVO

Konkrete materiell-rechtliche Vorgaben für die „spezifischeren Vorschriften" i. S. d. Art. 88 Abs. 1 DSGVO ergeben sich aus Art. 88 Abs. 2 DSGVO. Nach Art. 88 Abs. 2 DSGVO sollen die Vorschriften, die die Mitgliedstaaten nach Art. 88 Abs. 1 DSGVO vorsehen können, Maßnahmen zur Wahrung der berechtigten Interessen und Grundrechte der betroffenen Personen, insbesondere im Hinblick auf die Transparenz der Verarbeitung, umfassen.

Hinter diesen Vorgaben – so arbeitet es *Wünschelbaum* anhand der Prinzipientheorie von *Alexy* [467] heraus – verbirgt sich ein prinzipielles Schutzniveau.[468] Nach diesem sind die in den Art. 5, 6, 9 DSGVO verankerten Regelungsprinzipien zu beachten. Diese müssen die Betriebsparteien bei einer datenschutzrechtlichen Kollektivvereinbarung wahren. [469] Die Datenschutzgrundsätze aus Art. 5 DSGVO sollten als Optimierungsgebote und Auslegungshilfen herangezogen werden.[470] Aus ihnen ergibt sich etwa, dass eine Datenverarbeitung immer zweckgebunden sein muss (Art. 5 Abs. 1 lit. b DSGVO). Nach Art. 6 und 9 DSGVO ist eine Datenverarbeitung nur unter bestimmten Voraussetzungen zulässig. Abwägungsoffene Kriterien wie etwa das Merkmal der „Erforderlichkeit" setzen voraus, dass man das Interesse der betroffenen Person am Schutz ihrer personenbezogenen Daten sowie das Interesse der Verantwortlichen an der Datenverarbeitung gegeneinander abwägt. Daraus ergibt sich das Prinzip, dass die Betriebsparteien den Verhältnismäßigkeitsgrundsatz bei der Gestaltung datenschutzrechtlicher Kollektivvereinbarungen zu beachten haben.[471] Hinter Art. 7, 8 DSGVO verbergen sich hingegen keine übergeordneten Prinzipien. [472] Vielmehr enthalten sie Bedingungen zur Wirksamkeit der Einwilligung, die nicht in eine

[467] *Alexy*, Theorie der Grundrechte, 1994, S. 71 ff.

[468] *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 95 ff.; im Ergebnis auch: EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 14; a. A. BAG, 8 AZR 209/21 (A), NZA 2023, 363, 366.

[469] *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 99.

[470] *Ebd.*, S. 97 m. w. N.

[471] *Ebd.*, S. 98.

[472] *Ebd.*, S. 98.

Abwägung einbezogen werden. Sie werden daher nicht von Art. 88 Abs. 2 DSGVO erfasst.

Über das soeben dargestellte Konzept des prinzipiellen Schutzniveaus hinaus müssen die Betriebsparteien sich an den Art. 12 ff. DSGVO orientieren.[473] Die „Transparenz" der Verarbeitung ist in Art. 88 Abs. 2 DSGVO besonders hervorgehoben. Dieser gesetzgeberischen Entscheidung muss bei der Vereinbarung von Kollektivvereinbarungen Rechnung getragen werden. Art. 12 DSGVO enthält Vorgaben dazu, *wie* die Verantwortliche die betroffene Person gem. Art. 13, 14, 15 bis 22 und 34 DSGVO informieren soll. Demnach soll die Verantwortliche die Informationen, die sie der betroffenen Person nach den eben genannten Vorschriften zur Verfügung stellt, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln. Diese Vorgaben sind Ausprägung des Grundsatzes transparenter Datenverarbeitung nach Art. 5 Abs. 1 lit. a DSGVO.

c) Konsequenz: Art. 88 Abs. 1 DSGVO enthält kein „Abweichungsverbot"

Der Wortlaut des Art. 88 Abs. 1 DSGVO ist nicht eindeutig hinsichtlich der Reichweite der Öffnungsklausel und spricht somit weder für noch gegen die Zulässigkeit einer Abweichung „nach unten" oder „nach oben" durch Betriebsvereinbarungen.[474]

Nicht überzeugend ist es indes, sämtliche Normen der DSGVO einer Disposition durch Kollektivvereinbarungen zu entziehen. Die Entstehungsgeschichte des Art. 88 Abs. 2 DSGVO zeigt, dass sich der Unionsgesetzgeber bewusst dagegen entschieden hat, die Formulierung „in den Grenzen dieser Verordnung" in den Wortlaut aufzunehmen.[475]

Ein extensives Schutzniveau würde zudem darauf hinauslaufen, dass die Kollektivparteien vom Schutzstandard der DSGVO gar nicht abweichen

---

[473] *Ebd.*, S. 101.
[474] Sehr ausführlich dazu: *ebd.*, S. 45 ff.
[475] *Ebd.*, S. 93.

dürften.[476] Wenn die Kollektivparteien ohnehin alle Vorschriften in der DSGVO berücksichtigen müssten, hätten sie keinen Gestaltungsspielraum mehr.[477] Gerade diesen Gestaltungsspielraum soll aber Art. 88 Abs. 1 DSGVO gewährleisten.[478] Die Kollektivparteien sollen mit der Betriebsvereinbarung eigenständige Regelungs- und Lösungsansätze verfolgen können:[479] Eine Betriebsvereinbarung als kollektivrechtliche Regelung ist das Ergebnis von Verhandlungen paritätischer Parteien. Die finale Betriebsvereinbarung ist somit dadurch gekennzeichnet, dass im Zuge der Verhandlung die Belange beider Parteien hinreichend berücksichtigt wurden. Eine Partei kann sich bewusst auf eine für sie nachteilige Regelung einlassen, wenn dafür an anderer Stelle eine für sie vorteilhafte Regelung in den Vereinbarungstext aufgenommen wird. Etwa könnte vereinbart werden, dass auf der einen Seite zulasten der Arbeitnehmerinnen ein algorithmisches System im Bewerbungsverfahren eingesetzt wird und auf der anderen Seite zu deren Gunsten Arbeit im Home-Office flexibel möglich ist. Verböte Art. 88 Abs. 1 DSGVO, vom Schutzstandard der DSGVO in bestimmten Fällen abzuweichen, würde den Parteien die Möglichkeit genommen, zu verhandeln.

Die Gesetzeshistorie spricht zudem dafür, dass Abweichungen – sowohl „nach unten“ als auch „nach oben“ – möglich sind:[480] Mit dem Wortlaut der „spezifischere[n]“ Vorschriften wollten sich die Mitgliedstaaten einen Gestaltungsspielraum sichern.[481] Diesem Gestaltungsspielraum setzt lediglich

---

[476] *Ebd.,* S. 95.

[477] *Ebd.,* S. 95.

[478] *Ebd.*, S. 95.

[479] *Bissels/Meyer-Michaelis/Schiller*, DB 2016, 3042, 3048; *Düwell/Brink*, NZA 2017, 1081, 1082; *Franzen*, NZA 2020, 1593, 1595; vgl. *Plote*, Arbeitsrecht im Zeitalter der Digitalisierung, S. 93, 112, die Regelungen seien sonst „bloße Lippenbekenntnisse“.

[480] Taeger/Gabel/*Zöll*, Art. 88 DSGVO Rn. 17; sehr ausführlich dazu: *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 51 ff.

[481] *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 55.

Art. 88 Abs. 2 DSGVO „einen Rahmen".[482] Die in Art. 88 Abs. 2 DSGVO normierten Vorgaben wären obsolet, würde man stets ohne Einschränkungen das nach Art. 5 ff. DSGVO vorgegebene Schutzniveau wahren müssen.[483] Zudem wäre der Hinweis auf eine transparente Verarbeitung in Art. 88 Abs. 2 DSGVO überflüssig, würden die Art. 12 ff. DSGVO uneingeschränkt gelten.[484]

Auch bedeutet die *ASNEF*-Entscheidung[485] nicht zwingend, dass eine vollharmonisierende Wirkung auch im Bereich des Beschäftigtendatenschutzes erzielt werden soll. Die Entscheidung war insofern ein Sonderfall, als im spanischen Datenschutzrecht der Verhältnismäßigkeitsgrundsatz weitgehend abbedungen wurde.[486] Vielmehr bestätigt der EuGH mit seinem Urteil v. 30. März 2023, dass die Mitgliedstaaten innerhalb des von Art. 88 Abs. 2 DSGVO vorgegebenen Rahmens „zusätzliche, strengere oder einschränkende nationale Vorschriften" vorsehen können.[487] Zwar führt der EuGH nicht explizit aus, ob unter „zusätzliche" Vorschriften auch solche fallen, die „nach unten" vom Schutzstandard der DSGVO abweichen. Jedenfalls schließt die Formulierung eine Abweichung „nach unten" nicht aus. Dass der EuGH das Adjektiv „zusätzlich" aufgenommen hat, deutet vielmehr in die Richtung, dass er „nach unten" abweichende Vorschriften auch erfassen wollte. Ansonsten hätte er es

---

[482] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 662; *Nebel*, ZD 2018, 520, 523; *Wurzberger*, ZD 2017, 258, 263; *Wybitul*, NZA 2017, 1488, 1489, der den Streit für die Praxis als eher bedeutungslos einstuft, weil im Vordergrund die Schaffung maßgeschneiderter, rechtsicherer und transparenterer Vorgaben stehe; ErfK/*Kania*, § 87 BetrVG Rn. 61; Taeger/Gabel/*Zöll*, Art. 88 DSGVO Rn. 21

[483] *Thüsing/Granetzny*, Beschäftigtendatenschutz, 3. Aufl. 2021, § 4 Rn. 15.

[484] *Düwell/Brink*, NZA 2017, 1081, 1082; *Traut*, RDV 2016, 312, 314; *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 58.

[485] EuGH, 24.11.2011 – C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito ASNEF [C-468/10]; Federación de Comercio Electrónico y Marketing Directo FECEMD [C-469/10] ./. Administración del Estado*, NZA 2011, 1409.

[486] *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 77.

[487] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat ./. Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 661 Rn. 51.

bei der Formulierung „strengere oder einschränkende nationale Vorschriften“ belassen können.

3. Zwischenergebnis: Betriebsvereinbarung als flexible Rechtsgrundlage

1. Betriebsvereinbarungen können als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen.[488] Die Parteien können dabei vom prinzipiellen Schutzstandard des Art. 88 Abs. 2 DSGVO sowohl „nach unten“ als auch „nach oben“ abweichen.[489] Sie müssen die in Art. 5, 6, 9 DSGVO verankerten Prinzipien wahren und Art. 12 ff. DSGVO berücksichtigen.

2. So ist der durch Art. 88 Abs. 1 DSGVO bezweckte Gestaltungsspielraum gesichert, der es ermöglicht, dass die Parteien eine individuelle Vereinbarung für ihren Betrieb abschließen, die als Rechtsgrundlage für die Datenverarbeitung dient. [490] Die Betriebsparteien können selbst am besten einschätzen, welche Datenverarbeitungen im konkreten Fall angemessen sind. [491] Zudem setzt man durch den Abschluss von Betriebsvereinbarungen die Mitbestimmungsrechte des Betriebsrats um.[492] Sie werden deshalb auch bei den Arbeitnehmerinnen besonders akzeptiert.[493] Anders als bei einer Einwilligung als Erlaubnistatbestand besteht auch nicht das Risiko, dass aufgrund eines Widerrufs die Rechtsgrundlage für die zukünftige Datenverarbeitung entzogen wird.[494]

---

[488] *Holthausen*, RdA 2021, 19, 32.

[489] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 661 Rn. 51.

[490] Vgl. *Plote*, Arbeitsrecht im Zeitalter der Digitalisierung, S. 93, 109 f.; *Klösel/Mahnhold*, NZA 2017, 1428, 1431; *Wünschelbaum*, Kollektivautonomer Datenschutz, 2022, S. 100.

[491] *Plote*, Arbeitsrecht im Zeitalter der Digitalisierung, S. 93, 111.

[492] Richardi/*Maschmann*, § 87 BetrVG Rn. 77 ff.

[493] *Stück*, ZD 2019, 256, 257.

[494] *Raif*, in: Kramer (Hrsg.), Kramer IT-ArbR, 2019, C. IV. 1. Rn. 198.

3. Im Ergebnis ist die Betriebsvereinbarung somit das „zweckmäßigste und rechtssicherste Mittel [...], den Datenschutz am Arbeitsplatz belastbar und transparent zu regeln."[495]

D. Ergebnis des Systems als Grundlage für die Auswahlentscheidung

Wenn ein Ergebnis eines algorithmischen Systems generiert wurde, wird es von den Arbeitgeberinnen als Grundlage für Auswahlentscheidungen verwendet werden. Die Verarbeitung der personenbezogenen Daten beruht – wie eben ausgeführt – auf einer Rechtsgrundlage.[496] Das wird im konkreten Beschäftigungsverhältnis § 26 Abs. 1 S. 1 oder 2 BDSG oder eine Betriebsvereinbarung sein.

Neben der Voraussetzung, dass eine Rechtsgrundlage für die Verarbeitung der entsprechenden personenbezogenen Daten vorliegt, muss zudem Art. 22 Abs. 1 DSGVO berücksichtigt werden, wenn das generierte Ergebnis des algorithmischen Systems verwendet wird. Art. 22 Abs. 1 DSGVO ist eine zusätzliche Rechtmäßigkeitsvoraussetzung.[497]

Nach Art. 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtlich wirkt oder sie in ähnlicher Weise erheblich beeinträchtigt. Wenn ein algorithmisches System ein Ergebnis generiert, ob eine Person eingestellt, befördert oder gekündigt wird, kann es sich dabei um eine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung handeln, die gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Auf die einzelnen Voraussetzungen des Art. 22 Abs. 1 DSGVO wird im folgenden

---

[495] *Imping*, DB 2021, 1808, 1814; *Wybitul*, NZA 2017, 1488, 1494; *Köllmann*, Implementierung elektronischer Überwachungseinrichtungen durch Betriebsvereinbarung vor dem Hintergrund der DSGVO, 2021, S. 464 f.

[496] Kapitel 6 C. (S. 161).

[497] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 29.

Abschnitt näher eingegangen. Besondere Aufmerksamkeit wird dem Merkmal der „Ausschließlichkeit“ gewidmet: Wie groß muss der Handlungs- und Bewertungsspielraum des Menschen sein, der sich mit den Ergebnissen des algorithmischen Systems auseinandersetzt? Liegt eine ausschließliche Entscheidung nicht schon allein deshalb vor, weil durch die Ergebnisse die Person, die die Entscheidung über die Bewerberinnen oder Arbeitnehmerinnen trifft, derart beeinflusst ist, dass eine tatsächliche Bewertung, losgelöst von den Ergebnissen des Systems, nicht mehr stattfinden kann?

In der Literatur gibt es keine Ausführungen dazu, wie das Verhältnis von Art. 88 Abs. 1 DSGVO zu Art. 22 Abs. 1 DSGVO ist. Es ist aber davon auszugehen, dass es sich bei Art. 22 Abs. 1 DSGVO um eine Regelung handelt, von der die Betriebsparteien nicht abweichen dürfen. Zwar gehört sie nicht zu den in Art. 88 Abs. 2 DSGVO genannten Vorschriften, die als Rahmen für die spezifischeren Vorschriften nach Art. 88 Abs. 1 DSGVO gelten.[498] Art. 22 Abs. 1 DSGVO enthält aber eine grundlegende Wertung der DSGVO, die auch im Rahmen spezifischer Vorschriften nach Art. 88 Abs. 1 DSGVO berücksichtigt werden muss.

I. Historie von Art. 22 DSGVO

1. Art. 15 DSRL als Vorgängervorschrift zu Art. 22 DSGVO

Bereits Art. 15 DSRL[499] sah vor, dass „jede[...] Person das Recht [hat], keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens“.

In Art. 15 Abs. 2 DSRL waren Ausnahmen von Art. 15 Abs. 1 DSRL vorgesehen: Eine Person konnte nach Art. 15 Abs. 2 DSRL einer

---

[498] S. Kapitel 6 C.V.2.b) (S. 199).

[499] Richtlinie 95/46/EG (Abl. L 281 vom 23.11.1995).

Entscheidung nach Art. 15 Abs. 1 DSRL unterworfen werden, sofern diese im Rahmen des Abschlusses oder Erfüllung eines Vertrags ergeht (lit. a) oder durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt (lit. b).

Diese Ausnahmen wurden in Art. 22 Abs. 2 DSGVO übernommen, jedoch sieht Art. 22 Abs. 2 DSGVO auch eine Ausnahme vor, wenn eine ausdrückliche Einwilligung der betroffenen Person vorliegt (Art. 22 Abs. 2 lit. c DSGVO). Außerdem enthält Art. 22 DSGVO auch die Absätze 3 und 4, die in Art. 15 DSRL noch nicht vorkamen. Art. 22 Abs. 3 DSGVO sieht vor, dass die Verantwortliche in Fällen des Art. 22 Abs. 2 lit. a und c DSGVO angemessene Maßnahmen treffen soll, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. In Art. 22 Abs. 4 DSGVO ist normiert, dass Entscheidungen nach Art. 22 Abs. 2 DSGVO nicht auf besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO beruhen dürfen, sofern nicht ein Ausnahmetatbestand nach Art. 9 Abs. lit. a oder g DSGVO gilt und zudem angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der Person getroffen wurden.

2. Umsetzung von Art. 15 DSRL durch Art. 6a BDSG a. F.

Der deutsche Gesetzgeber hatte Art. 15 DSRL mit Art. 6a BDSG a. F. umgesetzt. [500] In § 6a BDSG a. F. wurde das Verbot automatisierter Entscheidungen auf Fälle begrenzt, in denen automatisierte Verfahren der Bewertung einzelner Persönlichkeitsmerkmale dienen. § 6a BDSG a. F. war richtlinienkonform.[501] Die Richtlinie hat es den Mitgliedstaaten überlassen, wie sie das in Art. 15 DSRL umgeschriebene Recht in nationales Recht umsetzen.[502]

---

[500] § 6a eingef. m. W. v 23.5.2001 durch G v. 18.5.2001 (BGBl. I S. 904).
[501] NK-BDSG/*Scholz*, § 6a BDSG Rn. 5 ff.
[502] NK-BDSG/*ders.*, § 6a BDSG Rn. 6.

Mit Erlass der DSGVO wurde § 6a BDSG a. F. von Art. 22 DSGVO abgelöst. Das Verbot ausschließlich automatisierter Entscheidungen gibt es daher schon länger. Es gibt allerdings kaum Rechtsprechung zu der Vorschrift.[503]

II. Rechtsnatur des Art. 22 Abs. 1 DSGVO

Art. 22 DSGVO ist in Kapitel 3 „Rechte der betroffenen Person" aufgeführt. Gem. Art. 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Dem Wortlaut und der systematischen Stellung zufolge ist Art. 22 Abs. 1 DSGVO den Betroffenenrechten zuzuordnen.[504]

Teilweise wird Art. 22 DSGVO auch als unabhängiges Verbot automatisierter Einzelentscheidungen verstanden.[505] Mit diesem Verständnis könnten am ehesten effektiv die Persönlichkeitsrechte der betroffenen Personen geschützt werden.[506]

Die dogmatische Einordnung des Art. 22 Abs. 1 DSGVO ist nicht entscheidend[507]: Zumindest mittelbar kommt der Norm Verbotscharakter zu[508], sodass es in der Praxis auf ein Verbot hinausläuft. Der mittelbare Verbotscharakter ergibt sich daraus, dass gem. Art. 83 Abs. 5 lit. b DSGVO ein Bußgeld von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von

---

[503] SCHUFA-Urteil zu § 6a BDGS a. F.: BGH, 28.1.2014 – VI ZR 156/13, NJW 2014, 1235.

[504] EuArbRK/*Franzen*, Art. 22 DSGVO Rn. 3; Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 1.

[505] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 2; NK-Datenschutzrecht/*Scholz*, Art. 22 DSGVO Rn. 1; Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 29b; *Krügel/Pfeiffenbring*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 11 Rn. 39.

[506] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 29b; *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 128.

[507] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 5; zur Einordnung als sozio-technische Gestaltungsnorm s. *Djeffal*, DuD 2021, 529.

[508] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 5.

bis zu 4 % des erzielten Jahresumsatzes droht, wenn gegen Art. 22 DSGVO verstoßen wird.

III. Telos: Schutz vor automatisierten Entscheidungen

1. Bezug zur Menschenwürde nach Art. 1 Abs. 1 GG

In der deutschen Literatur wird der Schutzzweck von Art. 22 DSGVO häufig dadurch aufgezeigt, dass auf die zur Menschenwürde nach Art. 1 Abs. 1 GG entwickelte Objektformel Bezug genommen wird[509]: Die betroffenen Personen sollen nicht einem „rein technischen und undurchschaubaren Vorgang ausgeliefert [sein]"[510] und „nicht zum bloßen Objekt einer mithilfe von Algorithmen gewonnen Bewertung ihrer persönlichen Daten gemacht werden"[511]. Die Objektformel wurde vom BVerfG entwickelt, um den Schutzgehalt der Menschenwürde zu erfassen.[512] Das Unionsrecht ist zwar grundsätzlich autonom auszulegen.[513] Allerdings ist der Wortlaut des Art. 1 GRCh fast identisch mit dem des Art. 1 Abs. 1 GG. Die Objektformel kann daher zumindest entsprechend herangezogen werden.[514]

2. Besonders hohes Risiko durch automatisierte Entscheidungen

Art. 15 DSRL wurde aus dem Grund in die DSRL aufgenommen, weil Datenschutz gleichermaßen für automatisierte und für nicht automatisierte Verarbeitung gelten muss: Das Schutzniveau darf nicht bei manueller und automatisierter Verarbeitung unterschiedlich sein.[515] Aus dem Amtsblatt geht aber nicht hervor, warum gerade eine Entscheidung, die auf einer

---

[509] *Hartmann/Kriebel*, DSRITB 2021, 129, 140; *Malorny*, JuS 2022, 289, 295.

[510] NK-Datenschutzrecht/*Scholz*, Art. 22 DSGVO Rn. 3.

[511] NK-Datenschutzrecht/*ders.*, Art. 22 DSGVO Rn. 3; vgl. *Malorny*, JuS 2022, 289, 296; *Steege*, MMR 2019, 715, 719.

[512] S. etwa BVerfG, 12.11.1997 – 1 BvR 479/92, 1 BvR 307/94, BVerfGE 96, 375; BVerfG, 15.12.1970 – 2 BvF 1/69, 2 BvR 629/68, 2 BvR 308/69, juris, Rn. 81; kritisch dazu: *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 193.

[513] S. etwa EuArbRK/*Franzen*, Art. 153 AEUV Rn. 5.

[514] S. Calliess/Ruffert/*Calliess*, Art. 1 GRCh Rn. 36.

[515] ABl. L 281 vom 23.11.1995, S. 33 Erwägungsgrund (27).

ausschließlich automatisierten Datenverarbeitung beruht, unzulässig ist. Ein eindeutiger gesetzgeberischer Wille ist nicht erkennbar.

Allerdings kann man dem geänderten Vorschlag der Kommission für eine Richtlinie für die Verarbeitung personenbezogener Daten[516] entnehmen, was die Beweggründe für einen solchen Artikel waren. Zu Art. 16 DSRL mit der Überschrift „Automatisierte Einzelentscheidungen"[517] wurde ausgeführt, dass die „Gefahr einer mißbräuchlichen Verwendung der Informatik bei der Entscheidungsfindung (...) eine der Hauptgefahren der Zukunft [ist]: Das von der Maschine gelieferte Ergebnis, die [sic, Bezug wohl auf Maschine] immer höher entwickelte Software und Expertensystemen zugrundelegt, hat einen scheinbar objektiven und unbestreitbaren Charakter, dem der menschliche Entscheidungsträger übermäßige Bedeutung beimessen kann, wenn er seiner Verantwortung nicht nachkommt"[518]. Mit Art. 22 Abs. 1 DSGVO drückt der Unionsgesetzgeber aus, dass ausschließlich automatisierte Entscheidungen für betroffene Personen ein besonders hohes Risiko bergen.[519] Die Risiken, die mit einer automatisierten Entscheidung einhergehen, sind größer als bei menschlichen Entscheidungen. Dieser Aussage ist in dieser Pauschalität aber nicht zuzustimmen. Wie bereits herausgearbeitet worden ist[520], haben sowohl menschliche als auch automatisierte Entscheidungen Vor- und Nachteile.

Am Ende bleibt daher die Frage, ob eine ausschließlich automatisierte Entscheidung eine größere Gefahr ist als eine ausschließlich menschliche Entscheidung. Sind bei einer menschlichen Entscheidung die Personen nicht genauso einer „Black-Box" ausgeliefert wie bei einem maschinell lernenden

---

[516] Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM (92) 422 endg – SYN 287.

[517] In der finalen Fassung der Richtlinie veröffentlicht als Art. 15.

[518] Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM (92) 422 endg – SYN 287, S. 26.

[519] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 1; Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 2; *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 122 f.

[520] Kapitel 3 (S. 33).

System?[521] Ein gutes Beispiel sind Abitur-Noten oder auch Noten, die man im Studium erhält. Noten sind häufig das wichtigste Kriterium, wenn es um die Entscheidung geht, ob eine Person eingestellt wird. Eine finale Note setzt sich aus mehreren Teilnoten zusammen und kommt durch die subjektive Bewertung von Einzelpersonen zustande. Für die finale Note sind dabei mehr Faktoren als bloß die objektive Leistung einer Person ausschlaggebend. Die Entscheidungsträgerin, der die finale Note einer Person vorliegt, weiß nicht, unter welchen Umständen die Note zustande gekommen ist. Mithin ist es mit einer „Black-Box" vergleichbar, wie sich eine einzelne Note zusammensetzt. Der Wissenschaftsrat stellte 2004 fest, dass Schulnoten nur begrenzt vergleichbar und mit Blick auf das Leistungsniveau eingeschränkt transparent seien.[522] Genauso wenig, wie man versteht, wie einzelne Noten zustande kommen, versteht man, warum genau ein algorithmisches System eine Person als verlässlich oder weniger verlässlich eingestuft hat. Der entscheidende Unterschied bei der Notengebung besteht aber darin, dass man dem System der Notengebung *vertraut*, weil man es kennt. Jede ist zur Schule gegangen und hat für die Leistungen Noten erhalten. Es gibt Lehrpläne und allgemeine Vorgaben, was einer Schülerin im Laufe ihrer Schullaufbahn beigebracht werden muss. Gleiches gilt für das Studium. Zudem basiert das Notengebungssystem auch auf objektiv messbaren Faktoren wie z. B. Erwartungshorizonten und Bewertungssystemen. Es handelt sich um einen regulierten Bereich, dem man vertraut.

Ein solches Vertrauen existiert (noch) nicht hinreichend gegenüber algorithmischen Entscheidungssystemen. Vertrauen schafft man durch Transparenz.[523] Die Entscheidung muss für die betroffene Person nachvollziehbar und erklärbar sein. Hinzu kommt, dass auch die fortschreitende Regulierung ein Baustein für mehr Vertrauen ist. Die Vorgaben für Hochrisiko-KI-Systeme, die zukünftig aufgrund der KI-VO erfüllt sein müssen, sorgen dafür, dass KI-Systeme in allen Bereichen – sei es vom Training der KI-Systeme bis hin zur fortlaufenden Überwachung – bestimmte Anforderungen erfüllen müssen. Andernfalls können sie nicht

---

[521] Vgl. dazu auch: *Wischmeyer*, AöR 143 (2018), 1, 54.

[522] *Wissenschaftsrat*, Empfehlungen zur Reform des Hochschulzugangs, 2004, S. 4; vgl. auch *BT-Drs. 15/3475*, S. 6.

[523] Kapitel 4 (S. 39).

eingesetzt werden. Das Vertrauen wird konkret auch durch ein Recht auf Erklärung der individuellen Entscheidung gem. Art. 68c KI-VO-PARL gestärkt.[524] Dieses Recht besteht dann, wenn eine Person einer Entscheidung unterworfen wurde, die auf Grundlage eines KI-Systems getroffen wurde.[525]

IV. Anwendungsbereich des Art. 22 Abs. 1 DSGVO bei algorithmischen Systemen in der Personalauswahl

1. Teleologische Reduktion des Merkmals „Entscheidung"

Art. 22 Abs. 1 DSGVO erfasst Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen. Der Begriff der Entscheidung ist in der DSGVO nicht legaldefiniert. Eine Entscheidung liegt vor, wenn man zwischen mindestens zwei Optionen anhand wertender Kriterien eine Wahl trifft.[526] Bei wörtlicher Anwendung würden auch simple Entscheidungen wie z. B. die automatisierte Zuteilung eines Parkplatzes nach der Adresseingabe oder ein freiwilliger, einseitig von der Arbeitgeberin gewährter Fahrtkostenzuschuss unter Art. 22 Abs. 1 DSGVO fallen.[527] Das würde in der Praxis dazu führen, dass jede Datenverarbeitung unter Art. 22 Abs. 1 DSGVO fällt.

Vorgeschlagen wird daher, das Merkmal der Entscheidung teleologisch zu reduzieren[528]: Teilweise wird vertreten, dass es sich bei der Entscheidung um eine personenbezogene Bewertung handeln müsse.[529] Andere sind der Auffassung, dass die Entscheidung zumindest ein „Mindestmaß an

---

[524] Kapitel 11 F. (S. 386).

[525] S. dazu näher unter: Kapitel 11 F. (s. S. 386).

[526] Sydow/Marsch/*Helfrich*, Art. 22 DSGVO Rn. 43.

[527] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 19; *Abel*, ZD 2018, 304, 305; *Chiba*, Dako 2020, 85, die vorschlägt, positive, ausschließlich auf automatisierter Verarbeitung beruhende Entscheidungen vom Anwendungsbereich des Art. 22 DSGVO herauszunehmen.

[528] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 19; Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 15c; vgl. BeckOK Datenschutzrecht/*v. Lewinski*, Art. 22 DSGVO Rn. 9 ff.

[529] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 15c; BeckOK Datenschutzrecht/*v. Lewinski*, Art. 22 DSGVO Rn. 9; *Abel*, ZD 2018, 304, 305.

Komplexität" aufweisen müsse.[530] Nach vorgegebenen Regeln getroffene „Wenn-Dann-Entscheidungen" seien nicht erfasst.[531]

a) Personenbezogene Bewertung

Die Vorgängerregelung in Art. 15 DSRL begrenzte den Anwendungsbereich auf Entscheidungen, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergehen, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

Auch wenn Art. 22 Abs. 1 DSGVO in seiner jetzigen Fassung die Einschränkung der automatisierten Verarbeitung zum Zwecke der Bewertung einer natürlichen Person nicht mehr beinhaltet, spricht Erwägungsgrund 71 S. 1 DSGVO für eine solche Einschränkung: „Die betroffene Person soll das Recht haben, keiner Entscheidung [...] zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden." Als Beispiel wird in Erwägungsgrund 71 S. 1 DSGVO die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahrens genannt.

Gegen eine Begrenzung des Anwendungsbereichs auf personenbezogene Bewertungen spricht aber, dass Art. 22 Abs. 1 DSGVO das Profiling hervorhebt. Profiling ist nach Art. 4 Nr. 4 DSGVO jede automatisierte Verarbeitung personenbezogener Daten, die darauf gerichtet ist, bestimmte persönliche Aspekte einer natürlichen Person zu bewerten, um etwa deren Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren oder auf dieser Grundlage vorherzusagen. Wenn personenbezogene Bewertungen durchgeführt werden, handelt es sich daher um Profiling. Dadurch, dass das Profiling hervorgehoben wird, wird deutlich, dass es sich beim Profiling um das wohl praktisch wichtigste

---

[530] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 19; Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 18.

[531] NK-Datenschutzrecht/*Scholz*, Art. 22 DSGVO Rn. 18; Kühling/Buchner/*Buchner*, Art. 22 Rn. 18.

Anwendungsbeispiel einer ausschließlich automatisierten Entscheidung handelt. Der Anwendungsbereich soll sich im Umkehrschluss nicht auf personenbezogene Bewertungen beschränken, sondern jegliche Art von Entscheidungen erfassen. Es sind dennoch kaum Entscheidungen denkbar, die nicht auf der Auswertung persönlicher Merkmale beruhen und damit zu personenbezogenen Bewertungen führen.[532] Jedenfalls bei den untersuchten algorithmischen Systemen, die im Personalwesen eingesetzt werden, werden häufig personenbezogene Merkmale ausgewertet.[533]

b) Mindestmaß an Komplexität der Entscheidung

Damit eine Entscheidung i. S. d. Art. 22 Abs. 1 DSGVO vorliegt, muss sie *Steinbach* zufolge ein Mindestmaß an Komplexität aufweisen, etwa mit einer dem Profiling vergleichbaren Analyse oder Vorhersage in Bezug auf die Eigenschaften oder Lebenssituation der betroffenen Person.[534]

Erfolge die Entscheidung anhand vorher festgelegter „Wenn-Dann-Regeln", liege keine Entscheidung i. S. d. Art. 22 Abs. 1 DSGVO vor.[535] Wenn ein solches Ergebnis anhand vorher festgelegter Parameter automatisiert entstehe, fehle es an einer erforderlichen autonomen Bewertung.[536] Als Beispiel dient folgendes Szenario: Eine Arbeitgeberin möchte aufgrund der Vielzahl der Bewerberinnen oder Arbeitnehmerinnen ein algorithmisches System einsetzen, um die Personen zunächst aufgrund „objektiver" Kriterien wie etwa der Noten oder Arbeitsleistung hinsichtlich der Anzahl der erledigten Projekte zu sortieren. Das algorithmische System sortiert anhand der vorgegebenen Merkmale die Personen. Kandidatinnen, die nicht den vorgegebenen

---

[532] *Brkan*, Int J Law Info Tech 27 (2019), 91, 97.

[533] S. dazu auch: Kapitel 2 (S. 23).

[534] *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 118 f.

[535] *Braegelmann/Kaulartz*, in: Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 392; Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 18; *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 119; a. A. Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 15b; *Blum*, People Analytics, 2021, S. 155.

[536] Vgl. BeckOK Datenschutzrecht/*v. Lewinski*, Art. 22 DSGVO Rn. 13; *Braegelmann/Kaulartz*, in: Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 393; a. A. Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 15b.

Hochschulabschluss erreichen oder die Mindestanzahl an Projekten erledigt haben, werden aussortiert.

Solche Entscheidungen vom Anwendungsbereich des Art. 22 Abs. 1 DSGVO auszunehmen, überzeugt. Der Mensch würde in solchen Fällen keine andere Auswahl treffen als die Maschine.[537] Eine Entscheidung i. S. d. Art. 22 Abs. 1 DSGVO ist daher nur anzunehmen, wenn etwa wie beim Profiling eine Analyse oder Vorhersage bestimmter Eigenschaften oder Situationen der betroffenen Person erfolgt.[538] Nur in dem Fall greift der Schutzzweck der Norm: Art. 22 Abs. 1 DSGVO soll verhindern, dass der Mensch einer automatisierten Entscheidung „ausgeliefert" ist. Die betroffene Person ist nicht ausgeliefert, wenn die Parameter für die Entscheidung vorher im Einvernehmen festgelegt worden sind.

2. Unterworfensein der betroffenen Person

Der Betroffene muss der Entscheidung *unterworfen* werden. Das Merkmal ist erfüllt, wenn eine Dritte einseitig Regeln für ein algorithmisches System vorgibt, die die Nutzerin nicht selbstständig regulieren kann.[539] Das bedeutet, dass Arbeitnehmerinnen oder Bewerberinnen einer Entscheidung unterworfen sind, wenn sie auf den Entscheidungsprozess keinen Einfluss haben.

3. Entscheidung beruht ausschließlich auf automatisierter Verarbeitung

a) Ausschließlichkeit der automatisierten Verarbeitung

Der Anwendungsbereich von Art. 22 DSGVO ist eröffnet, wenn die Entscheidung *ausschließlich* auf einer automatisierten Verarbeitung beruht. Eine automatisierte Entscheidung ist ausschließlich, wenn eine (Teil-)Bewertung oder Mitbestimmung einer natürlichen Person nicht stattfindet.[540] Das Merkmal der Ausschließlichkeit entfällt mithin immer

---

[537] *Götz*, Big Data im Personalmanagement, 2020, S. 167; i. E. auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 287.

[538] *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 119.

[539] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 24c.

[540] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 11.

dann, sobald die Letztentscheidung von einem Menschen getroffen wird.[541] Diskutiert wird die Frage, welche Qualität das „Dazwischentreten" des Menschen haben muss, damit die Entscheidung nicht ausschließlich auf der automatisierten Verarbeitung beruht.[542] Jedenfalls muss es möglich sein, von dem auf der automatisierten Verarbeitung beruhenden Ergebnis abzuweichen.[543] Seine Mitwirkung darf sich nicht auf einen bloß formalen Akt beschränken, vielmehr muss es sich um ein „qualifiziertes Dazwischentreten"[544] handeln. Wenn der Mensch die automatische Vorgabe übernimmt und ohne eigene Erwägungen umsetzt, ist das Merkmal der Ausschließlichkeit hingegen erfüllt.[545] Die Herausforderung liegt darin, sicherzustellen, dass ein Mensch die Auswahl tatsächlich überdenkt: Wie kann man nachvollziehen, dass ein Mensch eigene Erwägungen angestellt hat und nicht bloß die Vorgabe des algorithmischen Systems übernommen hat?

Werden Entscheidungen vorstrukturiert, sind sie vom Anwendungsbereich des Art. 22 Abs. 1 DSGVO nach überwiegender Ansicht nicht erfasst.[546] Algorithmische Systeme, die im Personalwesen eingesetzt werden, fallen mithin nicht in den Anwendungsbereich des Art. 22 Abs. 1 DSGVO, wenn sie Vorentscheidungen treffen. Das ist etwa dann der Fall, wenn das algorithmische System Rankings der Bewerberinnen oder der zu befördernden

---

[541] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 17b; *Hartmann/Kriebel*, DSRITB 2021, 129, 132.

[542] *Brkan*, Int J Law Info Tech 27 (2019), 91, 101 f.; *Hartmann/Kriebel*, DSRITB 2021, 129, 132; vgl. *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 116 f.

[543] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 13.

[544] S. dazu die Ausführungen von *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 134.

[545] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 15; NK-Datenschutzrecht/*Scholz*, Art. 22 DSGVO Rn. 26; *Knitter*, Digitale Weisungen, 2022, S. 116.

[546] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 16; Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 12; *Schwarze*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 8 Rn. 32; *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 121 f.; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 301.

Personen erstellt und keine konkrete Person vorschlägt, die eingestellt oder befördert werden soll.[547]

b) Gefahr auch bei einer bloßen Entscheidungsunterstützung

Im EU-Parlament wurde im Laufe des Gesetzgebungsverfahrens der DSGVO das Merkmal der Ausschließlichkeit diskutiert. Man erkannte die Gefahr teilweise automatisierter Verarbeitungen: „Auch eine nur teilweise automatisierte Verarbeitung und Bewertung eines bestimmten Sachverhalts birgt die Gefahr, dass wesentliche Aspekte unberücksichtigt bleiben und der Betroffene dadurch erhebliche Nachteile erleidet."[548]

Bereits zu § 6a BDSG a.F. wurde in der Gesetzesbegründung ausgeführt, dass die Vorgaben der Norm nicht dadurch umgangen werden können, „indem dem automatisierten Datenverarbeitungsverfahren, auf das sich die Entscheidung [...] stützt, noch eine mehr oder minder formale Bearbeitung durch einen Menschen nachgeschaltet wird, dieser Mensch aber gar keine Befugnis oder ausreichende Datengrundlage besitzt, um von der automatisierten Entscheidung abweichen zu können"[549]. Auch *Hoffman-Riem* sieht die Gefahr, dass bei einer Entscheiderin, die die Algorithmen kaum durchschauen und rekonstruieren könne, die „menschliche Prüfung und gegebenenfalls Ratifizierung des algorithmenfundierten Ergebnisses [sich] als praktisch weitgehend wirkungslos [...] erweisen"[550]. Es gibt z. B. einen Anbieter eines maschinell lernenden Systems zur Kandidatinnensuche, bei dem der Arbeitgeberin nach Abschluss des Bewerbungsprozesses eine Übersicht der Kandidatinnen präsentiert wird, die die einzelnen Persönlichkeitsprofile enthält.[551] Die Übersicht gibt an, wie gut eine Person zum Team und zu den Aufgaben passt. Kann man wirklich von einer

---

[547] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 188.

[548] *EP-LIBE-Ausschuss*, Änderungsanträge (5), S. 34.

[549] *BT-Drs. 16/10529*, S. 13.

[550] *Hoffmann-Riem*, AöR 142 (2017), 1, 36; vgl. dazu auch: *Brkan*, Int J Law Info Tech 27 (2019), 91, 101 f.

[551] Vgl. Angebot von *Retorio*: https://perma.cc/D63P-TN54 (archiviert am 02.08.2022).

eigenständigen Entscheidung sprechen, wenn die Arbeitgeberin die Ergebnisse auch nach einer Abwägung mehr oder weniger übernimmt?

Die Europäische Kommission hatte bereits 1992 in ihrem Vorschlag zur DSRL aufgeführt, dass die Ergebnisse der automatisierten Verarbeitung nicht die einzige Grundlage für die Entscheidung des Menschen sein dürften. Lehne eine Arbeitgeberin die Bewerberin aufgrund der Ergebnisse eines „psychotechnischen Computertests" ab, stehe die Ablehnung im Widerspruch zum Grundsatz einer erforderlichen menschlichen Beurteilung.[552] Gleiches gelte, wenn die Bewerberinnen in eine bestimmte Reihenfolge auf Grundlage eines Persönlichkeitstest eingeordnet würden. Mit dieser Argumentation würde auch die oben als zulässig aufgeführte Vorauswahl als unzulässig gelten, wenn ein Ranking von Personen erstellt wird. Warum bei einer derartigen Vorauswahl kein Raum für eine menschliche Beurteilung bleibt, führt die Europäische Kommission aber nicht weiter aus.

Bevor erläutert wird, wie man sicherstellen kann, dass die menschliche Entscheiderin tatsächlich eine eigene Entscheidung vornimmt, wird aufgezeigt, dass der Unterschied zwischen voll- und teilautomatisierten Entscheidungen im Ergebnis nicht groß ist. *Steinbach* zeigt das in ihrer Arbeit unter anderem an zwei verhaltenspsychologischen Effekten auf: der sog. Ankereffekt und ein übermäßiges Vertrauen in algorithmische Systeme (engl. *overreliance*).[553] Diese Effekte werden kurz vorgestellt.

aa) Ankereffekt

Der Ankereffekt taucht häufig im Zusammenhang mit numerischen, willkürlich vorgegebenen Ausgangswerten auf und beschreibt das Phänomen, dass sich Menschen an den Ausgangswerten orientieren.[554] *Tversky* und *Kahnemann* haben folgendes Experiment durchgeführt, um den Ankereffekt

---

[552] KOM(92) 422 endg. – SYN 287, Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, S. 27.

[553] *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 128.

[554] *Tversky/Kahneman*, Sciene, New Series 1974, 1124, 1128; *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 128.

zu zeigen:[555] Die Probanden sollten zu verschiedenen Fragen Schätzungen in Prozent angeben, wie groß der Anteil der afrikanischen Länder in der UNO ist. Vorher hatten sie an einem Glücksrad gedreht, welches eine Nummer zwischen 0 und 100 angezeigt hat. Dabei kam heraus, dass der zufällige Ausgangswert des Glücksrads die Beantwortung der Frage erheblich beeinflusst hatte: Die durchschnittliche Vermutung der Probandinnen schätzte den Prozentanteil der afrikanischen Länder in der UNO auf 25, wenn sie eine 10 gedreht hatten. Drehten sie eine 45, schätzten sie den Prozentanteil auf 65. Das Experiment zeigte: Die Menschen ließen sich von der vorher angezeigten Zahl beeinflussen, obwohl sie in keinem Verhältnis zur Fragestellung steht.

Bezogen auf algorithmische Systeme, die im Arbeitsverhältnis eingesetzt werden, werden sich die Personen, die die konkrete Entscheidung treffen, an den vom System vorgegebenen Ergebnissen orientieren. Eine Personalerin wird wohl kaum die Person einstellen, die vom algorithmischen System die schlechtesten Werte bekommen hat. Insofern kann man anzweifeln, ob nicht die tatsächliche Entscheidung im Endeffekt doch vom algorithmischen System vorgegeben, zumindest aber maßgeblich beeinflusst wird, sodass keine hinreichende menschliche Entscheidung mehr vorliegt.

bb) Overreliance

Hinzu kommt, dass man als Entscheidungsträgerin das Ergebnis des algorithmischen Systems womöglich als dem Menschen überlegene Entscheidungsfindung einordnet und dem algorithmischen System gewissermaßen blind „vertraut“ (engl. *overreliance*[556]).[557] Dieser Effekt – häufig auch „*automation bias*“[558] genannt – wird auch dadurch bestärkt, dass

---

[555] *Tversky/Kahneman*, Sciene, New Series 1974, 1124, 1128.

[556] *Baumgartner*, in: Bauer/Kechaja/Engelmann u.a. (Hrsg.), Diskriminierung und Antidiskriminierung, 2021, 160; *Hoffmann-Riem*, AöR 142 (2017), 1, 36.

[557] *Niehoff/Straker*, DSRITB 2019, 451, 455; *Bahner*, Übersteigertes Vertrauen in Automation: Der Einfluss von Fehlererfahrungen auf Complacency und Automation Bias, 2008, S. 40 ff.; vgl. *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 269.

[558] *Bahner*, Übersteigertes Vertrauen in Automation: Der Einfluss von Fehlererfahrungen auf Complacency und Automation Bias, 2008, S. 40 ff.

ein Mensch durch die von einer Maschine generierten Ergebnisse eine eigenständige Entscheidung und somit auch tatsächliche Verantwortung vermeiden kann.[559]

Ein maschinell lernendes System wurde mit einer Vielzahl an Daten trainiert und ist insofern „erprobt": Warum sollte es nicht die richtigen Schlüsse aus den Daten ziehen? Erkenntnisse aus Datenanalysen werden daher zum Teil als privilegierte Wissensquellen eingeordnet.[560] Auch im geänderten Vorschlag der Kommission für eine Richtlinie für die Verarbeitung personenbezogener Daten [561] wird darauf hingewiesen, dass die Entscheidungsträgerin dem maschinellen Ergebnis womöglich *übermäßige* Bedeutung zumisst.[562] Der Grund dafür liege in dem „scheinbar objektiven und unbestreitbaren Charakter"[563] des maschinellen Ergebnisses. Die Schlussfolgerungen, die bei maschinell lernenden Systemen aus Datensätzen gezogen werden, sind für die Menschen nicht ohne Weiteres nachvollziehbar.[564]

c) Lösung: Protokollpflicht

Ernst schlägt vor, eine Protokollpflicht [565] einzuführen, damit nachvollziehbar wird, dass die Letztentscheidungsbefugnis beim Menschen liegt.[566] Ähnlich wie bei der Anlageberatung bei Privatkunden (§ 83 Abs. 2 S. 1

---

[559] *Gigerenzer*, OBJEKT spektrum 2016, 6; *Niehoff/Straker*, DSRITB 2019, 451, 456.

[560] *Thapa*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, S. 268, 285.

[561] Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM (92) 422 endg – SYN 287.

[562] Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM (92) 422 endg – SYN 287, S. 26.

[563] Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM (92) 422 endg – SYN 287, S. 26.

[564] Kapitel 4 A.I.1. (S. 40).

[565] So auch: *Höpfner/Daum*, ZfA 2021, 467, 482; zu weiteren Lösungsmöglichkeiten s. *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 278 ff.

[566] *Ernst*, JZ 2017, 1026, 1031.

WpHG)[567] soll die Person, die die Entscheidung trifft, dokumentieren, dass sie die Entscheidung am Ende selbst getroffen hat. Dabei sieht *Ernst* auch die Gefahr, dass durch eine Protokollpflicht der Effizienzgewinn und Vorteil eines Algorithmeneinsatzes wieder verloren gehe. Allerdings sei angesichts der vielen rechtlichen Vorgaben, die an den Einsatz algorithmischer Systeme gestellt würden, ohnehin ein hoher Aufwand damit verbunden, das System möglichst rechtssicher zu gestalten. Eine weitere Protokollpflicht werde die Vorteile nicht aushebeln. Wie die Protokollpflicht genau ausgestaltet werden sollte, führt *Ernst* nicht näher aus.

Der Person, die die finale Entscheidung trifft, sollten vorher Kriterien an die Hand gegeben werden, die sie bei ihrer Entscheidung berücksichtigen soll. Nachdem die Person die Vorauswahl des algorithmischen Systems erhalten hat, sollte sie die Ergebnisse mithilfe der Kriterien auswerten. Dabei muss sie darlegen, warum im Einzelfall vom Ergebnis des algorithmischen Systems abgewichen wurde oder warum nicht. Die Erwägungen müssen dabei inhaltlich vollständig und für ausstehende Dritte nachvollziehbar sein. Eine sinnvolle Möglichkeit wäre es, einen Fragebogen für die jeweilige Auswahlentscheidung anzufertigen. Der Fragebogen könnte so aufgebaut sein, dass die Person kurz begründen muss, wie sie ihre Entscheidung getroffen hat. Für einen objektiven Dritten muss aus dem Fragebogen hervorgehen, dass die Person eigene Erwägungen mit in die Entscheidung hat einfließen lassen.

d) Zwischenergebnis zum Merkmal der Ausschließlichkeit

1. Rankings oder sonstige Vorschläge, die mithilfe einer automatisierten Datenverarbeitung erstellt werden, können als Grundlage für eine menschliche Entscheidung genutzt werden. Werden die Vorschläge ohne weitere Erwägungen übernommen, liegt eine ausschließlich automatisierte Entscheidung vor. Die Mitwirkung der Person, die

[567] *Ernst* bezog sich dabei noch auf die fast wortgleiche Vorgängervorschrift des § 34 Abs. 2a WpHG.

entscheidet, darf sich nicht auf einen bloß formalen Akt beschränken, vielmehr muss ein „qualifiziertes Dazwischentreten“ [568] vorliegen.

2. Die Analyse zeigt, dass auch bei einer bloßen Entscheidungsunterstützung das Risiko besteht, dass die Person sich von dem Ergebnis des algorithmischen Systems maßgeblich beeinflussen lässt und womöglich keine eigene Entscheidung mehr trifft.[569]

3. Um nachzuvollziehen, dass eine eigene Entscheidung getroffen wurde, kann eine Protokollpflicht eine Lösung sein. [570] Die Entscheidungsträgerin muss anhand eines Fragebogens beantworten, wie sie die Entscheidung getroffen hat. Für einen objektiven Dritten sollte aus den Ausführungen hervorgehen, dass eigene Überlegungen mit in die Entscheidung eingeflossen sind. Die Protokollpflicht kann verhindern, dass man gegen Art. 22 Abs. 1 DSGVO verstößt und es ggf. zu einer Bußgeldzahlung kommt. Sie ist daher eine praktikable Lösung, algorithmische Entscheidungsunterstützungssysteme rechtssicher zu implementieren.[571]

4. Rechtliche Wirkung oder erhebliche Beeinträchtigung

Bejaht man das Merkmal der Ausschließlichkeit, muss gem. Art. 22 Abs. 1 DSGVO die Entscheidung der betroffenen Person gegenüber rechtlich wirken oder sie in ähnlicher Weise erheblich beeinträchtigen.

Bezogen auf den Untersuchungsgegenstand ist daher die Frage, ob eine rechtliche Wirkung oder erhebliche Beeinträchtigung vorliegt, wenn ein algorithmisches System etwa Bewerberinnen aussortiert oder Arbeitnehmerinnen nicht für eine Beförderung vorschlägt.

---

[568] S. dazu die Ausführungen von *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 134.

[569] Kapitel 6 D.IV.3.b) (S. 216).

[570] Kapitel 6 D.IV.3.c) (S. 219).

[571] *Knitter*, Digitale Weisungen, 2022, S. 119.

a) Auslegung der Merkmale

Eine Entscheidung entfaltet nach überwiegender Auffassung rechtliche Wirkung, wenn konkrete Rechtsfolgen ausgelöst werden, d. h. eine Rechtposition begründet, geändert oder aufgehoben wird.[572] Im Privatrecht haben insbesondere rechtsgeschäftliche Willenserklärungen eine erhebliche rechtliche Wirkung, etwa wenn man ein Vertragsangebot annimmt oder einen Vertrag kündigt. [573] Keine rechtliche Wirkung liegt aber nach der überwiegenden Ansicht vor, wenn ein Vertrag nicht abgeschlossen wird: Der fehlende Abschluss rufe für die Person keine konkrete Rechtsfolge hervor.[574] Als Gegenargument nennt *Helfrich*, dass auch die Entscheidung, keinen Vertrag abzuschließen, den Status der Betroffenen ändere, da sie sich entscheide, in eine mögliche Rechtsbeziehung nicht einzutreten. [575] Eine Stellungnahme, ob eine rechtliche Wirkung vorliegt, wenn ein Vertragsschluss nicht zustande kommt, kann an dieser Stelle aber dahinstehen. Denn jedenfalls liegt in solchen Fällen eine erhebliche Beeinträchtigung in ähnlicher Weise vor, die ebenfalls von Art. 22 Abs. 1 DSGVO erfasst ist.[576]

Die Alternative der „erheblichen Beeinträchtigung in ähnlicher Weise“ in Art. 22 Abs. 1 DSGVO ist nicht als Auffangtatbestand zu verstehen, sondern steht gleichrangig neben der rechtlichen Folge. [577] Erheblich ist die Beeinträchtigung, wenn sie die Umstände, das Verhalten oder die Entscheidungen der betroffenen Person nachdrücklich beeinflusst, die betroffene Person über einen längeren Zeitraum oder dauerhaft belastet oder im schlimmsten Fall zum Ausschluss oder zur Benachteiligung der betroffenen Person führt. [578] Dazu gehören nach der Auffassung der Art. 29-

---

[572] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 24; Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 26; Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 21; *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 136.

[573] NK-Datenschutzrecht/*Scholz*, Art. 22 DSGVO Rn. 34.

[574] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 24; NK-Datenschutzrecht/*Scholz*, Art. 22 DSGVO Rn. 34.

[575] Sydow/Marsch/*Helfrich*, Art. 22 DSGVO Rn. 48.

[576] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 304.

[577] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 23.

[578] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 28.

Datenschutzgruppe neben Entscheidungen, die sich auf die finanzielle Lage einer Person auswirken, gerade auch solche, die den Zugang zu Arbeitsplätzen verwehren. [579] Das überzeugt, weil der Arbeitsplatz typischerweise eine erhebliche Bedeutung für die Finanzierung des Lebensalltags hat.

Die automatisierte Ablehnung von Bewerberinnen beeinträchtigt diese somit erheblich in ähnlicher Weise und ist von Art. 22 Abs. 1 DSGVO erfasst.

Das Argument, Art. 22 Abs. 2 DSGVO führe durch diese Auslegung zu einem faktischen Kontrahierungszwang, was insbesondere unter dem Blickwinkel der in Art. 2 Abs. 1 GG verankerten Privatautonomie[580] nicht tragbar wäre,[581] überzeugt nicht. Schließlich erlaubt es Art. 22 DSGVO durchaus, einen Vertrag nicht zu schließen. Verboten ist es nur, eine entsprechende Entscheidung ausschließlich aufgrund einer automatisierten Verarbeitung zu treffen.[582]

b) Positive Entscheidung auch erfasst

Fraglich ist, ob Art. 22 Abs. 1 DSGVO auch positive, begünstigende Entscheidungen erfasst. [583] Dann wäre es z. B. verboten, eine Beförderungsentscheidung ausschließlich automatisiert zu treffen. Der Wortlaut des Art. 22 Abs. 1 DSGVO unterscheidet nicht zwischen der Art der Entscheidung. Die Formulierung einer Beeinträchtigung legt jedoch nach dem allgemeinem Sprachverständnis eher etwas Nachteiliges nahe. [584] Allerdings wird in anderen Fassungen das Wort „*affect*" (engl.), „*afectar*" (span.) oder „*afecter*" (franz.) genutzt, das man am ehesten mit „beeinflussen" oder „sich auswirken" übersetzen kann.[585] Diese Begriffe erfassen vom Wortsinn her auch positive Entscheidungen. Weiter sind begünstigende Entscheidungen auch

---

[579] *Art. 29-Datenschutzgruppe*, WP251rev.01, S. 24.

[580] BVerfG, 27.7.2005 – 1 BvR 2501/04, NJW 2006, 596; Dürig/Herzog/Scholz/*Di Fabio*, Art. 2 Abs. 1 GG Rn. 101 f.

[581] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 23.

[582] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 26a.

[583] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 28.

[584] *Chiba*, Dako 2020, 85, 86.

[585] *Dies.*, Dako 2020, 85, 86 m. w. N.

vom Zweck der Vorschrift erfasst,[586] da jede Begünstigung einer Person für eine andere Person zu Nachteilen führen kann. Hätte der Gesetzgeber eine Ausnahme für solche Entscheidungen vorsehen wollen, hätte er eine Ausnahme nach Art. 22 Abs. 2 DSGVO aufführen können.

Eine Arbeitnehmerin wird demnach in ähnlicher Weise erheblich beeinträchtigt, wenn eine andere Arbeitnehmerin ausschließlich aufgrund einer automatisierten Entscheidung befördert wird. Etwas anderes kann wohl nur in Fällen gelten, in denen es keine anderen Personen gibt, die für die eine Beförderung in Betracht kämen, sodass dann keine Auswahlentscheidung vorliegt.

5. Ausnahmetatbestände nach Art. 22 Abs. 2 DSGVO

a) Entscheidung erforderlich für den Abschluss oder die Erfüllung eines Vertrags (Art. 22 Abs. 2 lit. a DSGVO)

Art. 22 Abs. 1 DSGVO gilt gem. Art. 22 Abs. 2 lit. a DSGVO nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und der Verantwortlichen erforderlich ist.

aa) Maßstab der Erforderlichkeit

Art. 6 Abs. 1 S. 1 lit. b und f DSGVO sowie § 26 Abs. 1 S. 1 BDSG enthalten auch das Merkmal der Erforderlichkeit, sodass es zunächst nahe liegt, für die Auslegung des Merkmals im Rahmen des Art. 22 Abs. 2 lit. a DSGVO ähnliche oder gar dieselben Erwägungen anzustellen.[587]

Allerdings muss gem. Art. 22 Abs. 2 lit. a DSGVO die *Entscheidung* erforderlich sein. Bei Art. 6 Abs. 1 S. 1 lit. b und f DSGVO sowie § 26 Abs. 1 S. 1 BDSG muss hingegen die *Verarbeitung* der personenbezogenen Daten erforderlich sein. Die unterschiedlichen Anknüpfungspunkte der Normen zeigen: Obwohl die Daten*verarbeitung* mit der anschließenden Entscheidung

---

[586] Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 28; a. A. *Chiba*, Dako 2020, 85, 87.

[587] *Meinecke*, Datenschutz und Data Science, 2021, S. 204; Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 30.

ein einheitlicher Prozess ist, trennt die DSGVO die beiden Vorgänge.[588] Für das Merkmal der Erforderlichkeit i. R. d. Art. 22 Abs. 2 lit. a DSGVO sollte daher nicht derselbe Maßstab angesetzt werden wie bei Art. 6 Abs 1 S. 1 lit. f DSGVO oder § 26 Abs. 1 BDSG.[589] Zwar verbirgt sich hinter dem Merkmal der Erforderlichkeit ebenfalls eine Verhältnismäßigkeitsprüfung. [590] Die Perspektive ist aber eine andere als etwa bei § 26 Abs. 1 S. 1 BDSG: Die Erforderlichkeit nach Art. 22 Abs. 2 lit. a DSGVO richtet sich danach, ob die *Entscheidung*, die auf einer *ausschließlich* automatisierten Verarbeitung beruht, geeignet, erforderlich und angemessen ist.[591]

Angesichts des grundsätzlichen Verbots einer ausschließlich automatisierten Entscheidung nach Art. 22 Abs. 1 DSGVO sind der Ausnahmetatbestand des Art. 22 Abs. 2 lit. a DSGVO und mithin auch das Merkmal der Erforderlichkeit eng zu verstehen.[592]

bb) Erforderlichkeit im Beschäftigungsverhältnis

Fraglich ist, ob Art. 22 Abs. 2 lit. a DSGVO im Beschäftigungskontext einschlägig ist. Die Möglichkeit, dass etwa ein Online-Einstellungsverfahren i. S. d. Art. 22 Abs. 2 lit. a DSGVO erforderlich ist, wird nicht bereits durch Erwägungsgrund 71 S. 1 DSGVO unmöglich. Erwägungsgrund 71 S. 1

---

[588] S. auch die Ausführungen zur Trennung in Verarbeitungsstadien: Kapitel 6 (S. 97).

[589] *Knitter*, Digitale Weisungen, 2022, S. 129; i. E. so wohl auch: Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 31a; *Wimmer* vertritt die Auffassung, dass die Erforderlichkeitsprüfung nach § 26 BDSG oder Art. 6 Abs. 1 lit. f DSGVO Indizwirkung für die Erforderlichkeitsprüfung nach Art. 22 Abs. 2 lit. a DSGVO entfaltet: *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 309.

[590] S. etwa *Art. 29-Datenschutzgruppe*, WP251rev.01, S. 25; a. A. Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 31a, der das Merkmal der Erforderlichkeit als „unvermeidlich" bzw. „unumgänglich" einordnet.

[591] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 28; Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 29; Sydow/Marsch/*Helfrich*, Art. 22 DSGVO Rn. 56; *Knitter*, Digitale Weisungen, 2022, S. 130; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 309; a. A. Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 31a, der sich nur auf „die Entscheidung" bezieht.

[592] Vgl. Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 28; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 310.

DSGVO nennt das Online-Einstellungsverfahren als Beispiel für eine unzulässige ausschließlich automatisierte Entscheidungsfindung. Dabei bezieht sich Erwägungsgrund 71 S. 1 DSGVO aber auf das Verbot ausschließlich automatisierter Entscheidung nach Art. 22 Abs. 1 DSGVO. Die Ausnahmen von Art. 22 Abs. 2 DSGVO bleiben unberührt.[593]

(1) Geeignetheit

Die ausschließlich automatisierte Entscheidung ist geeignet, wenn sie den verfolgten legitimen Zweck zumindest fördern kann. Im Beschäftigungskontext besteht der legitime Zweck darin, eine geeignete Bewerberin oder Arbeitnehmerin für die gesuchte Position zu finden. Solange ein algorithmisches System im Beschäftigungskontext eine für die gesuchte Position geeignete Person vorschlagen kann, fördert es den legitimen Zweck.

(2) Erforderlichkeit

Erforderlich ist die ausschließlich auf einer automatisierten Datenverarbeitung beruhenden Entscheidung, wenn kein gleich geeignetes, milderes Mittel ihr gegenüber besteht. Ein milderes Mittel ist angesichts des Schutzzwecks von Art. 22 Abs. 1 DSGVO eine Entscheidung, die nicht auf einer ausschließlich automatisierten Datenverarbeitung beruht. Das kann entweder eine menschliche Entscheidung sein oder eine Entscheidung, bei der ein algorithmisches System eine Vorauswahl trifft und final ein Mensch entscheidet. Eine menschliche Entscheidung ist nicht zwingend gleich geeignet wie die Entscheidung eines ausschließlich algorithmischen Systems.[594] Wenn allerdings eine automatisierte Vorauswahl getroffen wird und ein Mensch die finale Entscheidung trifft, kann es sich unter bestimmten Voraussetzungen um ein gleich geeignetes, milderes Mittel handeln. Die Kombination aus einer „Mensch-Maschine-Entscheidung“ ist in aller Regel besser geeignet als die ausschließlich automatisierte Entscheidung. Das liegt daran, dass der Mensch, der die Entscheidung final trifft, das Ergebnis der

[593] Vgl. dazu auch *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 318 f.; zweifelnd: Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 29.

[594] Vgl. *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 314 f.

Maschine unter anderen Gesichtspunkten als die Maschine bewerten kann. Schließlich entscheidet ein maschinell lernendes System ausschließlich auf Grundlage von Daten aus der Vergangenheit und kommt zu Ergebnissen mithilfe von Korrelationen und nicht auf der Grundlage von Kausalitäten.[595] Der Mensch ist hingegen in der Lage, seine Entscheidung spontan auch an neue Situationen anzupassen. Eine Kombination aus einer maschinellen Vorentscheidung und einer finalen menschlichen Entscheidung führt dazu, dass man die Nachteile von maschinellen und menschlichen Entscheidungen z. T. vermeiden kann und im Ergebnis zu einer gerechten Entscheidung kommt.

Gegenüber einer ausschließlich automatisierten Entscheidung ist die Kombination aus maschineller und menschlicher Entscheidung nur nicht gleich geeignet, wenn es „vernünftigerweise keine Alternative zu der automatisierten Entscheidungsfindung für die konkrete vertragliche Situation“[596] gibt. Das sind Fälle, in denen in kurzer Zeit eine Vielzahl von Verträgen geschlossen werden soll und daher eine Einschätzung – z. B. die Bonität die Vertragspartnerin betreffend – schnell feststehen muss. Die Ausnahme wird sich deshalb auf Massengeschäfte wie z. B. Bonitätsprüfungen für Darlehensverträge beschränken.[597] Ein Mensch ist in solchen Fällen gar nicht in der Lage, alle Entscheidungen auszuwerten. Im Beschäftigungskontext besteht ein Anwendungsfall, wenn es so viele Bewerberinnen gibt, dass eine menschliche Bewertung der Kandidatinnen bei einer bestimmten zeitlichen Vorgabe nicht umzusetzen wäre.[598] Das wird – wenn überhaupt – nur bei großen Unternehmen der Fall sein.[599]

Ernst sieht in der Argumentation die Gefahr, dass eine höhere Effizienz allein schon die Erforderlichkeit des Algorithmeneinsatzes begründet. Ansonsten

---

[595] S. dazu unter Kapitel 3 C. (S. 36).

[596] Braegelmann/Kaulartz/*Walter*, S. 396.

[597] Braegelmann/Kaulartz/*ders.*, S. 396; Spindler/Schuster/*Spindler/Horváth*, Art. 22 DSGVO Rn. 10.

[598] S. dazu ausführlich: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 152 ff.

[599] Bei *Google* haben sich im Jahr 2014 auf 6.000 Stellen drei Millionen Menschen beworben: *Akhtar/Gillett*, Business Insider, 12.04.2020, https://perma.cc/6LSN-QAQ4 (archiviert am 02.08.2022).

wäre faktisch jedes algorithmische System, das Arbeitgeberinnen aus Effizienzgründen verwenden, erforderlich.[600] Dabei wird aber übersehen, dass es nach zutreffender Argumentation für die Erforderlichkeit nicht darauf ankommt, ob das algorithmische System effizient ist, sondern darauf, ob die ausschließlich automatisierte Entscheidung das einzige Mittel ist, was der Menge an auszuwertenden Daten gerecht wird. Zwar spielt Effizienz dabei auch eine Rolle, sie ist aber nicht das ausschlaggebende Kriterium. Vielmehr ist das Kriterium der Erforderlichkeit nur erfüllt, wenn eine menschliche bzw. teilautomatisierte Entscheidung in der bestimmten Zeit nicht umgesetzt werden kann.

(3) Angemessenheit

Bei der Angemessenheit wird grundsätzlich eine Abwägung zwischen den Interessen der betroffenen Person und der Verantwortlichen vorgenommen. Die Verantwortliche hat ein Interesse an einer ausschließlich automatisierten Datenverarbeitung, während die betroffene Person hingegen daran interessiert ist, dass ihr Persönlichkeitsrecht nicht beeinträchtigt wird. Angesichts der engen Erforderlichkeitsprüfung überwiegt im Rahmen von Art. 22 Abs. 2 lit. a DSGVO in der Regel das Interesse an der ausschließlich automatisierten Entscheidung: Diese ist nur erforderlich, wenn es kein anderes Mittel gibt, die Entscheidung zu treffen. Das ist nur in solchen Fällen der Fall, in denen eine sehr große Datenmenge in kurzer Zeit ausgewertet werden muss, bei der es nicht möglich ist, Menschen zwischenzuschalten. In solchen Fällen käme es zu keiner Entscheidung, wenn keine ausschließlich automatisierte Entscheidung stattfinden würde.

Würde man die Angemessenheit verneinen, nachdem man die Erforderlichkeit im engeren Sinne bejaht hat, würde das dazu führen, dass man die Datenverarbeitung insgesamt nicht durchführen könnte. Schließlich braucht man ungeachtet von Art. 22 DSGVO eine Rechtsgrundlage für die Datenverarbeitung. Wenn die Anforderungen einer solchen Rechtsgrundlage erfüllt sind, würde Art. 22 DSGVO die Verarbeitung in dem Fall insgesamt unmöglich machen, wenn die Entscheidungsfindung nicht angemessen ist. Art. 22 DSGVO ist aber keine Verarbeitungsgrundlage. Die Vorschrift betrifft

[600] *Knitter*, Digitale Weisungen, 2022, S. 130.

nicht das „Ob“ der Datenverarbeitung, sondern das „Wie“ der Entscheidungsfindung.

Daher wird das Interesse an der Datenverarbeitung – auch im Interesse der betroffenen Person – überwiegen und die ausschließlich automatisierte Entscheidungsfindung auch angemessen sein, sofern sie denn im engeren Sinne erforderlich ist.

(4) Zwischenergebnis

Im Rahmen von Art. 22 Abs. 2 lit. a DSGVO wird geprüft, ob eine ausschließlich automatisierte Entscheidung erforderlich ist. Diese muss geeignet, erforderlich und angemessen sein.

Der Maßstab ist dabei aufgrund der Ausnahme zu Art. 22 Abs. 1 DSGVO eng zu verstehen. Im Beschäftigungskontext wird eine ausschließlich automatisierte Entscheidung nur erforderlich sein, wenn eine menschliche Entscheidung oder eine Kombination aus maschineller und menschlicher Entscheidung nicht realisierbar ist. Das wiederum setzt voraus, dass eine Entscheidung aus vielen Bewerberinnendaten oder Arbeitnehmerinnendaten innerhalb einer kurzen Zeitspanne getroffen werden muss.

b) Zulässigkeit aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten (Art. 22 Abs. 2 lit. b DSGVO)

Art. 22 Abs. 1 DSGVO gilt ebenfalls nicht, wenn gem. Art. 22 Abs. 2 lit. b DSGVO die Entscheidung aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten.

Eine mitgliedstaatliche Norm ist etwa § 37 BDSG, der automatisierte Einzelentscheidungen im Rahmen der Leistungserbringung nach einem Versicherungsvertrag erlaubt. Diese Norm ist aber für den Untersuchungsgenstand nicht relevant. Aktuell gibt es keine Erlaubnisnorm für automatisierte Entscheidungen im Beschäftigungsverhältnis.

c) Einwilligung der betroffenen Person (Art. 22 Abs. 2 lit. c DSGVO)

Schließlich gilt Art. 22 Abs. 1 DSGVO nicht, wenn gem. Art. 22 Abs. 2 lit. c DSGVO die Entscheidung mit ausdrücklicher Einwilligung der betroffenen Person erfolgt. Die Einwilligung muss sich ausdrücklich auf die konkrete Entscheidung aufgrund automatisierter Verarbeitung beziehen.[601]

aa) Maßstab analog Art. 4 Nr. 11, 6 Abs. 1 S. 1 lit. a, 7 Abs. 4 DSGVO und § 26 Abs. 2 BDSG

Die allgemeinen Vorschriften für die Einwilligung sind in Art. 4 Nr. 11, 6 Abs. 1 S. 1. lit. a und 7 DSGVO normiert. Diese Vorschriften beziehen sich auf die *Verarbeitung* personenbezogener Daten. Die Einwilligung in Art. 22 Abs. 2 lit. c DSGVO bezieht sich hingegen auf die ausschließlich automatisierte *Entscheidung*. Aus dem Grund kann man – wie bereits bei Art. 22 Abs. 2 lit. a DSGVO[602] – einen anderen Maßstab anlegen als bei sonstigen Einwilligungstatbeständen. Bei der Einwilligung sollte aber derselbe Maßstab wie auch bei der Einwilligung in die Datenverarbeitungen gelten: Die Anforderungen an die Einwilligung in die Verarbeitung personenbezogener Daten sollten nicht höher sein als die Anforderungen an die Einwilligung bei automatisierter Entscheidungsfindung.[603] Unabhängig vom Inhalt der Einwilligung – ob man nun in eine Verarbeitung oder eine Entscheidung einwilligt – schützen die Vorschriften die besondere Situation, in der sich die betroffene Person befindet. In beiden Situationen ist das Schutzbedürfnis der betroffenen Person gleich.[604]

In Arbeitsverhältnissen ist Art. 88 DSGVO zu berücksichtigen, sodass zusätzlich die Voraussetzungen des § 26 Abs. 2 BDSG eingehalten werden müssen.[605] Abgesehen vom Merkmal „Verarbeitung" müssen der sachliche

---

[601] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 31.

[602] Kapitel 6 D.IV.5.a)aa) (S. 224).

[603] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 41; *Braegelmann/Kaulartz*, in: Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 398, Rn. 19; *Knitter*, Digitale Weisungen, 2022, S. 134; a. A. *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 161.

[604] *Knitter*, Digitale Weisungen, 2022, S. 134.

[605] *Ders.*, Digitale Weisungen, 2022, S. 135; a. A. *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 161.

und persönliche Anwendungsbereich des § 26 BDSG eröffnet sein. Bei Auswahlentscheidungen im Bewerbungsverfahren oder bestehenden Arbeitsverhältnis werden personenbezogene Daten von Beschäftigten für Zwecke des Arbeitsverhältnisses verarbeitet. Auch der persönliche Anwendungsbereich erfasst nach § 26 Abs. 8 BDSG nicht nur Arbeitnehmerinnen, sondern auch Bewerberinnen (§ 26 Abs. 8 S. 2 BDSG). Der Anwendungsbereich von § 26 BDSG ist eröffnet.

Die Voraussetzungen für eine wirksame Einwilligung ergeben sich daher analog Art. 4 Nr. 11, 6 Abs. 1 S. 1 lit. a, 7 Abs. 4 DSGVO sowie § 26 Abs. 2 BDSG.[606]

bb) Einwilligung im Bewerbungs- und Beschäftigungsverhältnis

Anders als bei Art. 22 Abs. 2 lit. a DSGVO kann bei der Einwilligung nach Art. 22 Abs. 2 lit. c DSGVO auf die Ausführungen[607] im Rahmen von Art. 6 Abs. 1 S. 1 lit. a DSGVO und § 26 Abs. 2 BDSG verwiesen werden:[608] Es ist nicht möglich, die Datenverarbeitung mittels algorithmischer Systeme davon abhängig zu machen, ob ein Arbeitsverhältnis überhaupt begründet wird. Das widerspricht nicht nur Art. 7 Abs. 4 DSGVO, sondern schließt auch eine Freiwilligkeit insofern aus, als eine Wahlmöglichkeit nicht mehr besteht: Wenn die Datenverarbeitung für die Begründung des Arbeitsverhältnisses *erforderlich* ist, bleibt für eine echte Wahlmöglichkeit und somit eine Einwilligung kein Spielraum.[609]

Willigt die betroffene Person in die ausdrücklich automatisierte Entscheidung ein, geht es aber gerade darum, ob ein konkretes Beschäftigungsverhältnis oder eine neue Position im Unternehmen begründet wird. Es liegt somit in aller

---

[606] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 31; *Höpfner/Daum*, ZfA 2021, 467, 483; *Knitter*, Digitale Weisungen, 2022, S. 135; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 306; s. zu den Voraussetzungen im Einzelnen bereits unter: Kapitel 6 C.III. (S. 163).

[607] S. Kapitel 6 B.V. (S. 145); Kapitel 6 C.III. (S. 163).

[608] *Knitter*, Digitale Weisungen, 2022, S. 135; Braegelmann/Kaulartz/*Walter*, S. 398; a. A. *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 181.

[609] Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 203; Kühling/Buchner/*Maschmann*, Art. 88 DSGVO Rn. 51.

Regel ein Verstoß gegen Art. 7 Abs. 4 DSGVO vor. Die Ausnahme des Art. 22 Abs. 2 lit. c DSGVO ist somit im Beschäftigungskontext nicht relevant.[610]

6. Schutzmaßnahmen nach Art. 22 Abs. 3 DSGVO

Nach Art. 22 Abs. 3 DSGVO trifft die Verantwortliche in den in Art. 22 Abs. 2 lit. a und c DSGVO genannten Fällen angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Dazu gehört nach Art. 22 Abs. 3 DSGVO mindestens das Recht, dass eine Person seitens der Verantwortlichen eingreift, man seinen eigenen Standpunkt darlegen und die Entscheidung anfechten kann.

Wie sich die Vorgaben des Art. 22 Abs. 3 DSGVO zu den allgemeinen Informationspflichten nach Art. 12 ff. DSGVO verhalten, geht aus der Norm nicht hervor. *Schulz* hält das Zusammenspiel der Norm mit anderen, allgemeineren Vorgaben zu Informationspflichten gar für „misslungen".[611] Dem ist zuzustimmen: Die in Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g und 15 Abs. 1 lit. h DSGVO genannten spezifischen Rechte über die Existenz und Folgen einer automatisierten Entscheidungsfindung werden in den spezifischen Informationspflichtenkatalogen nicht weiter erwähnt.[612] In der Praxis bietet sich daher ein dreistufiges Verfahren an[613]: Die betroffene Person ist zunächst darüber zu informieren, dass eine automatisierte Entscheidung bestehe, welche Logik involviert sei und welche Tragweite und Auswirkungen die Verarbeitung für die betroffene Person mit sich bringe (Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g DSGVO)[614]. Außerdem muss die betroffene Person über ihre Rechte nach Art. 22 Abs. 3 DSGVO aufgeklärt werden. Im zweiten Schritt müssen der Person die wesentlichen Gründe der Entscheidung mitgeteilt werden: Nur wenn die Person weiß, welche Gründe der Entscheidung zugrunde liegen, kann sie weitere Rechte nach Art. 22 Abs. 3 DSGVO in

---

[610] Ähnlich auch: *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 307; *Jares/Vogt*, in: Knappertsbusch/Gondlach (Hrsg.), Arbeitswelt und KI 2030, 2021, 79; *Höpfner/Daum*, ZfA 2021, 467, 484.

[611] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 33; ähnlich auch: Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 32.

[612] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 33.

[613] Gola/Heckmann/*ders.*, Art. 22 DSGVO Rn. 34.

[614] Kapitel 7 B.III. (S. 250).

Anspruch nehmen.[615] Auf der dritten Stufe muss die betroffene Person die Möglichkeit bekommen, ggf. ein Recht nach Art. 22 Abs. 3 DSGVO geltend zu machen. Ein Recht auf Begründung der Entscheidung kann aber nicht pauschal bei jeder Art von algorithmischen Entscheidungen angenommen werden.[616] Hinzu kommt, dass ein solches Recht auch in rechtlicher und technischer Hinsicht nicht einfach umzusetzen ist. Im Hinblick auf das Recht auf Begründung ist auf die Ausführungen im Rahmen der Informationspflichten zu verweisen.[617]

Das Recht auf „Erwirkung des Eingreifens einer Person seitens des Verantwortlichen" umfasst, dass die automatisiert getroffene Entscheidung noch einmal von einem Menschen überprüft wird.[618] Daran fehlt es, wenn ein Fall des Art. 22 Abs. 2 DSGVO vorliegt, da in den Fällen das Verbot ausschließlich automatisierter Entscheidungsfindung nach Art. 22 Abs. 1 DSGVO nicht besteht.

Das Recht auf „Darlegung des eigenen Standpunkts" ist nicht so zu verstehen, dass es der betroffenen Person möglich ist, dass sie persönlich vorspricht. Vielmehr reicht es aus, dass eine postalische oder elektronische Adresse angegeben wird, an die sich die Person wenden kann.[619] Wichtig ist, dass der Standpunkt der betroffenen Person zur Kenntnis genommen wird und ggf. die Entscheidung geändert wird.[620]

Zudem nennt Art. 22 Abs. 3 DSGVO ein Recht auf Anfechtung der Entscheidung. Der Begriff der „Anfechtung" ist autonom unionsrechtlich auszulegen und nicht mit dem zivilrechtlichen oder verwaltungsrechtlichen Begriff gleichzusetzen.[621] Vielmehr versteht man unter dem Anfechtungsrecht das Recht der betroffenen Person, die Entscheidung überprüfen zu lassen.[622]

---

[615] *Knitter*, Digitale Weisungen, 2022, S. 143.

[616] S. dazu sogleich: Kapitel 7 B.V.3. (S. 259).

[617] S. zum Recht auf Begründung der Entscheidung unter: Kapitel 7 B.V.3. (S. 259).

[618] BeckOK Datenschutzrecht/*v. Lewinski*, Art. 22 DSGVO Rn. 48.

[619] BeckOK Datenschutzrecht/*ders.*, Art. 22 DSGVO Rn. 49.1.

[620] BeckOK Datenschutzrecht/*ders.*, Art. 22 DSGVO Rn. 49.1.

[621] BeckOK Datenschutzrecht/*ders.*, Art. 22 DSGVO Rn. 50.

[622] BeckOK Datenschutzrecht/*v. Lewinski*, Art. 22 DSGVO Rn. 50; Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 31.

Überprüfen muss die Entscheidung die Verantwortliche.[623] In der Praxis wird es aber wohl nur zu einer tatsächlichen Neuentscheidung kommen, wenn etwa bestehende Benachteiligungsschutzmaßnahmen wie z. B. Vorschriften aus dem AGG missachtet worden sind. Im Privatrechtsverhältnis – also auch im Arbeitsverhältnis – besteht ansonsten kein Zwang, eine Entscheidung zu ändern.[624]

V. Ergebnis zu Art. 22 DSGVO

1. Art. 22 DSGVO regelmäßig nicht einschlägig

Wenn algorithmische Systeme unterstützend bei der Entscheidungsfindung eingesetzt werden, sind sie von Art. 22 Abs. 1 DSGVO nicht erfasst.[625] Art. 22 Abs. 1 DSGVO verbietet nur ausschließlich auf einer automatisierten Datenverarbeitung beruhende Entscheidungen.

Trotzdem sind automatisiert generierte Vorschläge, die zur Unterstützung der Entscheidung herangezogen werden, ebenfalls gefährlich.[626] Die Personen, die die Auswahlentscheidung treffen, werden von der Vorentscheidung beeinflusst sein. Sichergestellt werden muss daher, dass die Entscheidungsträgerinnen noch tatsächlich eine eigene Entscheidung vornehmen. Übernehmen die Entscheidungsträgerinnen ohne weitere Abwägung das Ergebnis der maschinellen Datenverarbeitung, liegt eine ausschließlich automatisierte Entscheidung vor. Daher müssen die Entscheidungsträgerinnen ihre Entscheidung in einem Protokoll festhalten, aus dem hervorgeht, welche Kriterien sie der Entscheidung zugrunde gelegt haben und warum sie die Schlüsse aus der Vorentscheidung so gezogen haben, dass sie zu dem bestimmten Ergebnis gekommen sind. Es bietet sich an, dass die Entscheidungsträgerinnen diese Punkte anhand eines Fragebogens abarbeiten. Die verantwortliche Person kann so nachweisen, dass tatsächlich

---

[623] Kühling/Buchner/*Buchner*, Art. 22 DSGVO Rn. 31.

[624] Gola/Heckmann/*Schulz*, Art. 22 DSGVO Rn. 35; *Knitter*, Digitale Weisungen, 2022, S. 144.

[625] *Hoffmann-Riem* bezeichnet Art. 22 DSGVO daher als „stumpfes Schwert", s. *Hoffmann-Riem*, in: Unger/Ungern-Sternberg (Hrsg.), Demokratie und künstliche Intelligenz, 2019, 148.

[626] Kapitel 6 D.IV.3.b) (S. 216).

eine menschliche Bewertung und anschließende Entscheidung stattgefunden hat.

Von einer zukünftigen KI-VO werden auch solche Systeme erfasst, die bloß entscheidungsunterstützend eingesetzt werden. Nach Anhang III Nr. 4 lit. b KI-VO-PARL sind auch solche Systeme Hochrisiko-KI-Systeme, die Entscheidungen hinsichtlich Anbahnung, Beförderung und Beendigung von arbeitsbezogenen Vertragsverhältnissen wesentlich beeinflussen. Auch wenn Art. 22 Abs. 1 DSGVO in solchen Fällen nicht greift, werden dennoch zahlreiche Pflichten nach einer zukünftigen KI-VO auf die Anbieterinnen und Bereitstellerinnen zukommen.[627]

2. (Unsichere) Ausnahmen nach Art. 22 Abs. 2 DSGVO

Die Ausnahmen nach Art. 22 Abs. 2 DSGVO sind mit Blick auf Art. 22 Abs. 1 DSGVO eng auszulegen. Im Beschäftigungskontext wird eine Ausnahme nach Art. 22 Abs. 2 DSGVO fast nie einschlägig sein: Nach Art. 22 Abs. 2 lit. a DSGVO ist eine ausschließlich automatisierte Entscheidung nur erforderlich, wenn sie das einzige Mittel ist, um die Entscheidung zu treffen. Das ist im Beschäftigungskontext nur der Fall, wenn aus einer Vielzahl an Daten eine schnelle Entscheidung getroffen werden muss, die ein Mensch auch nicht mithilfe einer maschinellen Entscheidung treffen kann. Die Ausnahme nach Art. 22 Abs. 2 lit. b DSGVO ist im Beschäftigungskontext ebenfalls nicht einschlägig.

Eine Einwilligung in eine ausschließlich automatisierte Entscheidung gem. Art. 22 Abs. 2 lit. c DSGVO scheitert am Verstoß gegen Art. 7 Abs. 4 DSGVO. Ein Vertragsabschluss darf nicht davon abhängig sein, ob eine Einwilligung erteilt wurde oder nicht. Das wäre bei Art. 22 Abs. 2 lit. c DSGVO aber der Fall.

3. Rechte nach Art. 22 Abs. 3 DSGVO

Wenn eine Ausnahme nach Art. 22 Abs. 2 lit. a und c DSGVO einschlägig ist, muss die Verantwortliche die betroffene Person gem. Art. 22 Abs. 3

---

[627] Kapitel 10 (S. 341).

DSGVO über die zusätzlichen Rechte informieren. Diese in Art. 22 Abs. 3 DSGVO genannten Rechte treten neben die allgemeinen Informationspflichten der Art. 13 und 14 DSGVO. Da eine Einwilligung gem. Art. 22 Abs. 2 lit. c DSGVO im Bewerbungs- und Beschäftigungsverhältnis wegen eines Verstoßes gegen Art. 7 Abs. 4 DSGVO nicht möglich ist und eine Ausnahme gem. Art. 22 Abs. 2 lit. a DSGVO nur greift, wenn eine menschliche oder eine Kombination aus maschineller und menschlicher Entscheidung nicht realisierbar ist, ist der Anwendungsbereich des Art. 22 Abs. 3 DSGVO ohnehin nur selten eröffnet.

E. Zwischenergebnis: Rechtmäßigkeit der Datenverarbeitung

1. Werden personenbezogene Daten verarbeitet, muss eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen. Werden sensible Daten verarbeitet, ist die Verarbeitung grundsätzlich nach Art. 9 Abs. 1 DSGVO verboten, wenn nicht eine der in Art. 9 Abs. 2 DSGVO genannten Ausnahmen eingreift.

2. Der Anwendungsbereich der DSGVO indes ist nicht eröffnet, wenn anonyme Daten verarbeitet werden. Voraussetzung ist aber, dass die Daten auch *wirksam* anonymisiert sind, also der Personenbezug komplett aufgehoben und keine Re-Identifizierung mehr möglich ist. Es ist technisch schwierig, aus einem umfassenden personenbezogenen Datenbestand einen vollständig anonymen Datenbestand zu generieren.[628]

3. Der Vorgang des Anonymisierens selbst ist eine Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO, sodass eine Rechtsgrundlage dafür vorliegen muss. Sensible Daten können nur unter den zusätzlichen Voraussetzungen des Art. 9 Abs. 2 DSGVO anonymisiert werden.

---

[628] Vgl. *Winter/Battis/Halvani*, ZD 2019, 489; *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 10.04.2014, S. 5; s. dazu auch: *Ohm*, UCLA Law Rev. 2010, 1701.

4. Die Verantwortliche muss prüfen und dokumentieren, ob eine Anonymisierung technisch möglich ist. Ist sie technisch möglich, muss die Verantwortliche anonymisierte Daten verwenden, da sonst ein Verstoß gegen den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO vorliegt.

5. Art. 6 Abs. 4 DSGVO regelt die Weiterverarbeitung von Daten, die zu einem anderen Zweck als demjenigen erfolgt, der ursprünglich für die Verarbeitung vorgesehen war. Voraussetzung für die Weiterverarbeitung ist, dass der andere Zweck mit dem ursprünglichen Zweck vereinbar ist. Die Vereinbarkeit wird anhand einer umfassenden Einzelfallabwägung unter Berücksichtigung der in Art. 6 Abs. 4 lit. a-f DSGVO aufgeführten Kriterien beurteilt. Die Voraussetzungen des Art. 6 Abs. 4 DSGVO werden regelmäßig nicht erfüllt sein, sodass ein Training algorithmischer Systeme auf der Grundlage dieser Norm ausscheidet.[629]

6. Sensible Daten i. S. d. Art. 9 Abs. 1 DSGVO dürfen grundsätzlich nur nach den Ausnahmetatbeständen des Art. 9 Abs. 2 DSGVO verarbeitet werden. In Art. 6 Abs. 4 lit. c DSGVO werden sensiblen Daten gem. Art. 9 Abs. 1 DSGVO indes ausdrücklich genannt. Somit sind sensible Daten im Rahmen von Art. 6 Abs. 4 lit. c DSGVO ein Abwägungs- und kein sofortiges Ausschlusskriterium. Je sensibler allerdings die personenbezogenen Daten sind, desto eher ist eine Weiterverarbeitung unzulässig.

7. Für Trainingszwecke ist die Einwilligung keine rechtssichere Verarbeitungsgrundlage: Die betroffene Person kann ihre Einwilligung jederzeit widerrufen.[630] Das kann im Extremfall dazu führen, dass das ganze maschinell lernende System in der Form, wie es trainiert wurde, nicht mehr verwendet werden darf.

8. Verarbeitet man die personenbezogenen Daten zu Trainingszwecken auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f DSGVO, ist es ein milderes

---

[629] Kapitel 6 B.IV.4. (S. 137).
[630] Kapitel 6 B.V.3. (S. 151).

Mittel gegenüber der Verarbeitung personenbezogener Daten, wenn die Daten pseudonymisiert verarbeitet werden.[631] Im Übrigen dürfen im Rahmen des Art. 6 Abs. 1 S. 1 lit. f DSGVO die Interessen der betroffenen Personen nicht überwiegen. Das ist der Fall, wenn geeignete Schutzmaßnahmen für die relevanten Daten getroffen wurden.

9. Seit dem Urteil des EuGH vom 30. März 2023[632] ist § 26 Abs. 1 S. 1 BDSG nicht mehr anwendbar.[633] Werden personenbezogene Daten für ein konkretes Beschäftigungsverhältnis verarbeitet, ist nunmehr Art. 6 Abs 1 S. 1 lit. b DSGVO als Rechtsgrundlage heranzuziehen. Zentrales Merkmal des Art. 6 Abs. 1 S. 1 lit. b DSGVO ist die „Erforderlichkeit“[634].

10. Dabei muss ein maschinell lernendes System auf Ebene der Geeignetheit insbesondere eine hohe Qualität der Trainingsdaten aufweisen.[635] Zudem darf das algorithmische System nur zulässige Fragen in Bezug auf die konkrete Tätigkeit stellen.[636]

11. Auf Ebene der Erforderlichkeit darf es kein milderes, gleich geeignetes Mittel geben.[637] Je nach Anwendungsfall kann ein algorithmisches System sogar milder sein gegenüber herkömmlichen Verfahren zur Bewerberinnenvorauswahl oder Auswahl von Arbeitnehmerinnen, die z. B. befördert werden sollen.

12. Zuletzt muss der Einsatz eines algorithmischen Systems auch angemessen sein.[638] Dabei sind das Interesse der Arbeitgeberin an der Datenverarbeitung und das Persönlichkeitsrecht der betroffenen Person gegeneinander abzuwägen. Bei der Abwägung ist insbesondere zu

---

[631] Kapitel 6 B.VI.2.a) (S. 155).

[632] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[633] Kapitel 5 B.II.1.c) (S. 87).

[634] Kapitel 6 C.IV. (S. 171).

[635] Kapitel 6 C.IV.2.b)aa) (S. 176).

[636] Kapitel 6 C.IV.2.b)bb) (S. 177).

[637] Kapitel 6 C.IV.2.c) (S. 178).

[638] Kapitel 6 C.IV.2.d) (S. 182).

berücksichtigen, dass Arbeitnehmerinnen nicht permanent überwacht werden dürfen, eine umfassende Persönlichkeitsprofilerstellung unzulässig ist und der Person nicht ihre Individualität abgesprochen werden darf.[639]

13. Die Voraussetzungen einer Einwilligung der betroffenen Person werden für die Zwecke der Datenverarbeitung im konkreten Beschäftigungsverhältnis regelmäßig nicht erfüllt sein, da es an der Freiwilligkeit i. S. d. § 26 Abs. 2 BDSG fehlen wird.[640] Die Einwilligung kann außerdem jederzeit widerrufen werden, sodass die Verarbeitungsgrundlage *ex nunc* entfällt und die Daten gem. Art. 17 Abs. 1 lit. b DSGVO gelöscht werden müssen. Deshalb ist Einwilligung keine rechtssichere Rechtsgrundlage für die Datenverarbeitung im laufenden Beschäftigungsverhältnis.

14. Art. 88 Abs. 1 DSGVO räumt den Mitgliedstaaten im Beschäftigtendatenschutz eine autonome Regelungsbefugnis ein. Betriebsvereinbarungen können als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen.[641] Die Parteien können dabei richtigerweise vom prinzipiellen Schutzstandard des Art. 88 Abs. 2 DSGVO sowohl „nach unten" als auch „nach oben" abweichen.[642] Sie müssen die in Art. 5, 6 und 9 DSGVO verankerten Prinzipien wahren und Art. 12 ff. DSVO berücksichtigen.

15. Wenn algorithmische Systeme unterstützend bei der Entscheidungsfindung eingesetzt werden, sind sie nicht nach Art. 22 Abs. 1 DSGVO unzulässig.[643] Art. 22 Abs. 1 DSGVO verbietet nur

---

[639] Kapitel 6 C.IV.2.d)aa)(6) (S. 188).

[640] Kapitel 6 C.III.1. (S. 163).

[641] *Holthausen*, RdA 2021, 19, 32.

[642] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 661 Rn. 51; Kapitel 6 C.V.2. (S. 195).

[643] *Hoffmann-Riem* bezeichnet Art. 22 DSGVO daher als „stumpfes Schwert", s. *Hoffmann-Riem*, in: Unger/Ungern-Sternberg (Hrsg.), Demokratie und künstliche Intelligenz, 2019, 148.

ausschließlich auf einer automatisierten Datenverarbeitung beruhende Entscheidungen.

16. Trotzdem sind automatisiert generierte Vorschläge, die zur Unterstützung der Entscheidung herangezogen werden, ebenfalls gefährlich. [644] Die Personen, die die Auswahlentscheidung treffen, werden von der Vorentscheidung beeinflusst sein. Sichergestellt werden muss daher, dass die Entscheidungsträgerinnen noch tatsächlich eine eigene Entscheidung vornehmen. Diese Eigenentscheidung muss zudem nachweisbar sein, z. B. durch ein Entscheidungsprotokoll, aus dem die berücksichtigten Kriterien hervorgehen.

17. Die Ausnahmen nach Art. 22 Abs. 2 DSGVO sind mit Blick auf Art. 22 Abs. 1 DSGVO eng auszulegen. Im Beschäftigungskontext wird eine Ausnahme nach Art. 22 Abs. 2 DSGVO fast nie einschlägig sein, da die einzelnen Voraussetzungen nur in Ausnahmefällen vorliegen werden. [645]

---

[644] Kapitel 6 D.IV.3.b) (S. 216).
[645] Kapitel 6 D.V.2. (S. 235).

Kapitel 7

Weitere Pflichten der Verantwortlichen und Betroffenenrechte

Setzt man algorithmische Systeme zur Verarbeitung personenbezogener Daten ein, müssen neben den in den vorherigen Abschnitten erläuterten grundsätzlichen Rechtmäßigkeitsvoraussetzungen [1] auch weitere Pflichten eingehalten werden. Die Verantwortliche muss eine DSFA durchführen, wenn die Voraussetzungen des Art. 35 Abs. 1 DSGVO vorliegen. Außerdem muss sie die in Art. 13 und 14 DSGVO niedergelegten Informationspflichten wahren. Für algorithmische Systeme sind insbesondere Art. 13 Abs. 2 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO relevant.

Der betroffenen Person stehen hingegen gem. Art. 15 – Art. 21 DSGVO verschiedene Rechte zu.

Welche Herausforderungen sich bei den aufgezählten Pflichten und Betroffenenrechten im Kontext algorithmischer Systeme stellen, ist Gegenstand des nächsten Abschnitts.

A. DSFA gem. Art. 35 DSGVO bei algorithmischen Systemen erforderlich

Gem. Art. 35 Abs. 1 S. 1 DSGVO muss die Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen, wenn eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und

[1] Kapitel 6 (S. 97).

Freiheiten natürlicher Personen zur Folge hat. Gem. Art. 35 Abs. 2 DSGVO kann die Verantwortliche bei der Durchführung einer DSFA den Rat einer Datenschutzbeauftragen einholen, wenn eine solche benannt wurde. Auftragsverarbeiterinnen [2] sind nicht dazu verpflichtet, eine DSFA durchzuführen. Allerdings wird die Verantwortliche regelmäßig auf die Unterstützung der Auftragsverarbeiterin angewiesen sein, wenn sie die DSFA durchführt: Verarbeitet die Auftragsverarbeiterin die Daten, kann sie Art, Umfang, Umstände und Zwecke der Verarbeitung regelmäßig besser beurteilen als die Verantwortliche.[3]

Die DSFA ist keine Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten.[4] Eine unterlassene erforderliche DSFA oder eine fehlerhaft durchgeführte DSFA kann aber gem. Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt sein. Nicht sanktioniert wird, wenn die Abhilfemaßnahmen nicht ordnungsgemäß umgesetzt worden sind.[5] Diese müssen zur Bewältigung der identifizierten Risiken gem. Art. 35 Abs. 7 lit. d DSGVO in der DSFA enthalten sein.

Ob eine DSFA durchgeführt werden muss, ist davon abhängig, ob voraussichtlich ein hohes Risiko vorliegt. Der Risikobegriff wird von der DSK[6] aus den Erwägungsgründen 75 und 94 S. 2 DSGVO hergeleitet. Danach liegt ein Risiko vor, wenn es möglich ist, dass ein Ereignis eintritt, das selbst ein Schaden ist oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.[7] Ob ein hohes Risiko vorliegt, lässt sich anhand der Risikomatrix der DSK[8], der in Abs. 3 aufgeführten Fallgruppen und anhand einer von der DSK herausgegebenen Liste mit Verarbeitungstätigkeiten[9] einschätzen.

---

[2] Kapitel 6 A.I.2.b) (S. 101).

[3] Vgl. Gola/Heckmann/*Nolte/Werkmeister*, Art. 35 DSGVO Rn. 34.

[4] Ehmann/Selmayr/*Baumgartner*, Art. 35 DSGVO Rn. 78; *Schmitz/Dall'Armi*, ZD 2017, 57, 60; vgl. *Blum*, People Analytics, 2021, S. 169.

[5] Ehmann/Selmayr/*Baumgartner*, Art. 35 DSGVO Rn. 78.

[6] S. dazu: Kapitel 5 A.III.1.c) (S. 64).

[7] *Datenschutzkonferenz* (DSK), Kurzpapier Nr. 18, S. 1.

[8] *Dies.*, Kurzpapier Nr. 18, S. 5.

[9] *Dies.*, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 2018.

Demnach ist es erforderlich, beim Einsatz algorithmischer Systeme im Bewerbungsverfahren oder in bestehenden Arbeitsverhältnis eine DSFA durchzuführen. [10] Nach Art. 35 Abs. 3 lit. a DSGVO ist eine DSFA erforderlich, wenn es sich um eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen handelt, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen. Davon sind insbesondere Verarbeitungen erfasst, die die Kompetenz oder die Leistung einer Arbeitnehmerin bewerten sollen, wie etwa Assessmentverfahren, Beförderungsranglisten oder Computertests zur Bewerberinnenauswahl. [11] Der Liste der Verarbeitungstätigkeiten ist zu entnehmen, dass eine DSFA beim „Einsatz künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Bewertung persönlicher Aspekte der betroffenen Person" durchgeführt werden soll"[12]. Bei den untersuchten algorithmischen Systemen werden regelmäßig persönliche Aspekte einer betroffenen Person bewertet. KI wird in der Liste nicht weiter definiert. In einem Positionspapier der DSK vom 6.11.2019 [13] wird unter KI „die Anwendung von Verfahren des maschinellen Lernens und der Einsatz von KI-Komponenten verstanden, mit denen diese Verfahren umgesetzt werden". Mithin fallen algorithmische Systeme unter den KI-Begriff, die unter Einsatz maschinellen Lernens zustande gekommen sind.[14]

I. Datenschutzfolgenabschätzung als Instrument für Transparenz

Ziel der DSFA ist es, vor Beginn der Verarbeitung das Risiko der Verarbeitung einordnen zu können, um geeignete Abhilfemaßnahmen zu

---

[10] *Ebers/Heinze/Krügel/Steinrötter*, in: Künstliche Intelligenz und Robotik, 2020, S. 438 Rn. 83; *Kuß*, in: Kuß/Steege/Chibanguza (Hrsg.), Künstliche Intelligenz, 2022, 2. Teil § 6 G. Beschäftigtendatenschutz Rn. 69.

[11] Gola/Heckmann/*Nolte/Werkmeister*, Art. 35 DSGVO Rn. 22; Plath/*Bussche/Raguse*, Art. 35 DSGVO Rn. 27.

[12] *Datenschutzkonferenz* (DSK), Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 2018, S. 3.

[13] *Dies.*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 2019, S. 1.

[14] S. dazu bereits unter: Kapitel 1 C. (S. 12)

treffen.[15] Die Risiken der Verarbeitung sollen somit für die betroffenen Personen reduziert werden.[16] Die DSFA hilft bei der Erfüllung der Dokumentationspflichten aus der DSGVO und kann als wichtiger Bestandteil des Risikomanagements in Bezug auf den Datenschutz angesehen werden.[17] Die DSFA kann dazu beitragen, Auseinandersetzungen mit Aufsichtsbehörden und Betroffenen zu vermeiden.[18]

Verantwortliche können die DSFA vor allem als Möglichkeit sehen, Transparenz und damit auch Vertrauen[19] der betroffenen Personen bei der Datenverarbeitung zu gewinnen. Das kann vor allem dadurch umgesetzt werden, dass die Zusammenfassung und die Ergebnisse der DSFA veröffentlicht werden.[20] Eine explizite Pflicht zur Veröffentlichung der DSFA sieht die DSGVO nicht vor. Aus Betroffenenperspektive kann die DSFA aber als Ergänzung zu den Informationspflichten[21] eine Möglichkeit sein, einen detaillierten Überblick über die Risikobewertung und insbesondere die geplanten Abhilfemaßnahmen der Verantwortlichen zu erhalten. Eine Möglichkeit ist es etwa, bei den Informationspflichten auf die DSFA zu verweisen, damit die betroffene Person sich ggf. weitere Informationen einholen kann.

II. Durchführung der DSFA

1. Verarbeitungsverzeichnis gem. Art. 30 DSGVO

Gem. Art. 30 DSGVO muss die Verantwortliche ein Verarbeitungsverzeichnis führen, in dem alle relevanten Angaben über die Verarbeitung der Daten enthalten sind. Das Verarbeitungsverzeichnis ist

---

[15] BeckOK Datenschutzrecht/*Hansen*, Art. 35 DSGVO Rn. 1.

[16] Ehmann/Selmayr/*Baumgartner*, Art. 35 DSGVO Rn. 1.

[17] *Wybitul/Ströbel*, BB 2016, 2307, 2311.

[18] *Schmitz/Dall'Armi*, ZD 2017, 57, 64.

[19] S. dazu bereits unter: Kapitel 4 (S. 39).

[20] *Art. 29-Datenschutzgruppe*, Leitlinien zur DSFA und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248), S. 22; *Friedewald/Schiering/Martin*, DuD 2019, 473, 477; *Martini*, Blackbox Algorithmus, 2018, S. 210 ff.

[21] Dazu sogleich: Kapitel 7 B. (S. 117).

Ausgangspunkt der Verantwortlichen, um den Pflichten der DSGVO nachzukommen.[22] Im Verarbeitungsverzeichnis soll vermerkt werden, ob eine Datenschutzfolgenabschätzung durchgeführt wurde.[23]

2. Mindestinhalt der DSFA

Art. 35 Abs. 7 DSGVO gibt vor, was die DSFA enthalten muss. Inhaltlich müssen zumindest vier Punkte erfüllt sein, die in Vorbereitungsphase, Bewertungsphase und Maßnahmenphase eingeteilt werden können:[24]

- eine systematische Beschreibung der Verarbeitungsvorgänge und Zwecke der Verarbeitung ggf. einschließlich berechtigter Interessen der Verantwortlichen (Art. 35 Abs. 7 lit. a DSGVO);
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge bezogen auf den Zweck der Verarbeitung (Art. 35 Abs. 7 lit. b DSGVO);
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gem. Abs. 1 (Art. 35 Abs. 7 lit. c DSGVO) und
- geplante Abhilfemaßnahmen, um die Risiken zu bewältigen einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, die den Schutz personenbezogener Daten sicherstellen und den Nachweis erbringen, dass die Vorschriften der Verordnung eingehalten werden (Art. 35 Abs. 7 lit. d DSGVO).

3. Risikobewertung und geplante Maßnahmen zur Risikominimierung

Grundsätzlich gilt: Je größer die Risiken für die Rechte und Freiheiten natürlicher Personen sind, desto mehr Maßnahmen muss die Verantwortliche treffen, um das Risiko zu minimieren.[25] Bei algorithmischen Systemen, die im Bewerbungsverhältnis oder bestehenden Arbeitsverhältnis eingesetzt werden, besteht ein großes Risiko für die betroffene Person: Je nachdem, wie das Ergebnis ist, wird der Person ggf. der Zugang zu einer konkreten Stelle verweigert. Die Verantwortliche muss daher angemessene Garantien und

---

[22] *Dovas*, ITRB 2019, 14, 15.
[23] *Dies.*, ITRB 2019, 14, 15.
[24] Von dem Bussche/Voigt/*Koglin*, Teil 2 Kap. 5 Rn. 37.
[25] *Wybitul/Ströbel*, BB 2016, 2307, 2310.

Sicherheitsvorkehrungen treffen sowie nachweisen können, dass die Verarbeitung im Einklang mit den Vorschriften der DSGVO erfolgt. Beim Training algorithmischer Systeme kommen etwa die Möglichkeiten der Anonymisierung bzw. Pseudonymisierung in Betracht.[26]

4. Konsultationspflicht der Aufsichtsbehörde

Gem. Art. 36 Abs. 1 DSGVO konsultiert die Verantwortliche vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern die Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Die Vorschrift ist nicht so zu verstehen, dass die Verantwortliche immer bei einem hohen Risiko die Aufsichtsbehörde konsultieren muss, sondern nur, wenn dem hohen Risiko nicht bereits durch angemessene Maßnahmen begegnet wurde:[27] Ist nach Beendigung der DSFA das Risiko trotz der ergriffenen Maßnahmen weiterhin hoch, muss die Aufsichtsbehörde konsultiert werden.[28] Die Behörde kann Empfehlungen erteilen, insbesondere Vorschläge, um das Risiko einzudämmen.[29] Gem. Art. 83 Abs. 2 DSGVO kann die Aufsichtsbehörde auch die in Art. 58 DSGVO genannten Befugnisse nutzen, etwa auch die Verarbeitung vorübergehend oder endgültig beschränken (Art. 58 Abs. 2 lit. f DSGVO).[30]

B. Informationspflichten gem. Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO

Ein weiterer Grundsatz der Verarbeitung personenbezogener Daten ist gem. Art. 5 Abs. 1 lit. a DSGVO, dass die Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffenen Person nachvollziehbaren Weise verarbeitet werden.[31] Dieser Grundsatz wird auch durch die

---

[26] S. dazu bereits unter: Kapitel 6 B. (S. 117).

[27] *Dovas*, ITRB 2019, 14, 19.

[28] *Braun*, ZD 2021, 297, 298; *Dovas*, ITRB 2019, 14, 19.

[29] Gola/Heckmann/*Nolte/Werkmeister*, Art. 36 DSGVO Rn. 6.

[30] Gola/Heckmann/*dies.*, Art. 36 DSGVO Rn. 7.

[31] Zur Verbindlichkeit der Datenschutzgrundsätze s. Kapitel 6 A.IV (S. 114).

Informationspflichten nach Art. 13, 14 DSGVO erfüllt.[32] Neben den grundsätzlichen Informationspflichten nach Art. 13 Abs. 1 und Art. 14 Abs. 1 DSGVO muss die Verantwortliche die betroffene Person gem. Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO informieren, wenn sie die Daten zu einem anderen als dem ursprünglichen Zweck weiterverarbeiten will.[33] Verstöße gegen die Informationspflichten können mit Bußgeldern gem. Art. 83 Abs. 5 lit. b DSGVO geahndet werden.

Art. 13 DSGVO ist einschlägig, wenn personenbezogene Daten bei der betroffenen Person erhoben werden. Art. 14 DSGVO ist hingegen anwendbar, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. Vom Regelungsgehalt unterscheiden sich die beiden Artikel aber nur unwesentlich, sodass sie im folgenden Abschnitt zusammen abgehandelt werden. Modifiziert werden in Art. 14 DSGVO der Zeitpunkt der Mitteilung (Art. 14 Abs. 3 DSGVO) sowie die Ausnahmen wegen Unmöglichkeit oder Unverhältnismäßigkeit (Art. 14 Abs. 5 DSGVO).

Die Informationspflichten können dazu beitragen, mehr Transparenz[34] bei der Verarbeitung personenbezogener Daten zu schaffen und dadurch das Vertrauen in algorithmische Systeme zu steigern. Augenmerk des nächsten Abschnitts liegt auf Art. 13 Abs. 2 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO. Diese beiden Vorschriften sind beim Einsatz maschinell lernender Systeme besonders relevant: Nach den wortlautgleichen Vorschriften stellt die Verantwortliche aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zur Verfügung.

Im Folgenden wird herausgearbeitet, welchen Anwendungsbereich die beiden Informationspflichten haben[35], ob bereits der Zeitpunkt der Informationspflichten einen Hinweis auf ihren Inhalt gibt[36] und welche

---

[32] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 38 f.

[33] S. zur Zweckänderung unter: Kapitel 6 B.IV. (S. 133).

[34] Kapitel 4 (S. 39).

[35] Kapitel 7 B.I. (S. 248).

[36] Kapitel 7 B.II. (S. 249).

Vorgaben die Informationspflichten letztlich beinhalten[37]. Sodann wird darauf eingegangen, wie die Informationspflichten in der Praxis umgesetzt werden können.[38] Schließlich werden drei Vorschläge erläutert, wie die Informationspflichten *de lege ferenda* ausgestaltet werden können, um den Transparenzanforderungen hinreichend Rechnung zu tragen.[39]

I. Nur ausschließlich automatisierte Entscheidungen erfasst

Eine Informationspflicht besteht nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO *zumindest* für Fälle automatisierter Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1 und Abs. 4 DSGVO.[40]

Nach dem Wortlaut besteht die Informationspflicht an sich nicht bei Entscheidungen, die von einem algorithmischen System lediglich vorbereitet werden.[41] Das Wort „zumindest" kann man jedoch auch dahingehend verstehen, dass die Informationspflicht auch in anderen Fällen als in denen der ausschließlich automatisierten Entscheidungsfindung bestehen kann.[42] Versteht man die Normen so, bleibt jedoch die Frage offen, in welchen anderen Fällen die Informationspflicht besteht. Eine Informationspflicht müsste jedenfalls immer bestehen, wenn die Maßnahme ähnlich intensiv die Persönlichkeitsrechte der betroffenen Person berührt wie eine ausschließlich automatisierte Entscheidung.[43] Mithilfe dieser vagen Formel können die Fälle jedoch nicht sicher eingestuft werden.

Der Anwendungsbereich der Informationspflicht nach Art. 13 Abs. 2 lit. f. und Art. 14 Abs. 2 lit. g DSGVO umfasst somit nur die genannten Fälle der

---

[37] Kapitel 7 B.III. (S. 250).

[38] Kapitel 7 B.IV. (S. 253).

[39] Kapitel 7 B.V. (S. 257).

[40] Zu dem Verweis auf Art. 22 Abs. 1 und 4 DSGVO s. auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 342.

[41] *Martini*, Blackbox Algorithmus, 2018, S. 178; *Sesing*, MMR 2021, 288, 289; *Ebers*, in: Colonna/Greenstein (Hrsg.), Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence, 2022, S. 103, 109.

[42] Kühling/Buchner/*Bäcker*, Art. 13 DSGVO Rn. 52; *Sesing*, MMR 2021, 288, 290.

[43] *Martini*, Blackbox Algorithmus, 2018, S. 183.

ausschließlich automatisierten Entscheidung.[44] Eine bloße Vorauswahl der Bewerberinnen oder Arbeitnehmerinnen bei einer Beförderung ist keine solche ausschließlich automatisierte Entscheidung.[45] Auch wenn diese Informationspflicht somit für die bloße Entscheidungsunterstützung *de lege lata* nicht gilt und mithin für den Untersuchungsgegenstand der Arbeit kaum Bedeutung hat, wird der Inhalt der Informationspflicht erläutert. *De lege ferenda* sollten diese Informationspflichten nicht auf Fälle des Art. 22 Abs. 1 DSGVO begrenzt werden.[46]

II. Zeitpunkt der Informationspflichten nicht maßgeblich für den Inhalt

Die Informationspflichten nach Art. 13, 14 DSGVO greifen dem Wortlaut der jeweiligen Norm zufolge zu unterschiedlichen Zeitpunkten, weshalb vertreten wird, dass der Umfang der Informationspflichten variiert.[47] Art. 13 DSGVO bezieht sich vom Wortlaut auf den Zeitpunkt, wenn die Daten bei der betroffenen Person erhoben werden. Damit greifen die Informationspflichten zeitlich vor dem eigentlichen Verarbeitungsvorgang. Die Verantwortliche kann in dem Stadium noch nicht gem. Art. 13 Abs. 2 lit. f DSGVO über das konkrete Ergebnis informieren, sondern nur abstrakt über die Funktionen des Entscheidungssystems.[48]

Bei Art. 14 Abs. 2 lit. g DSGVO als auch der wortgleichen Vorschrift des Art. 15 Abs. 1 lit. h DSGVO gibt es keinen solchen eindeutigen Zeitpunkt. Nach Art. 14 Abs. 3 lit. a DSGVO muss die Verantwortliche die Informationen innerhalb einer angemessenen Frist, spätestens innerhalb eines Monats, nachdem sie die personenbezogenen Daten erlangt hat, erteilen. Art. 15 Abs. 1 DSGVO gewährt der betroffenen Person das „Recht, von der Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende

---

[44] *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 342 f.

[45] Dazu bereits: Kapitel 6 D.IV.3.a) (S. 214).

[46] S. dazu sogleich unter: Kapitel 7 B.V.1. (S. 257).

[47] Kühling/Buchner/*Bäcker*, Art. 15 DSGVO Rn. 15; Taeger/Gabel/*Mester*, Art. 15 DSGVO Rn. 12.

[48] *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018, S. 25; *Knitter*, Digitale Weisungen, 2022, S. 172; *Kumkar/Roth-Isigkeit*, JZ 2020, 277-286, 283 ff.

personenbezogene Daten verarbeitet werden", sodass nach dem Wortlaut die Auskunft sogar während des Verarbeitungsvorgangs selbst erteilt werden kann.[49]

Im Ergebnis unterscheiden sich die Informationspflichten nach Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g sowie 15 Abs. 1 lit. h DSGVO jedoch im Umfang:[50] Der Wortlaut der konkreten Informationspflicht über die involvierte Logik und die angestrebten Auswirkungen ist stets identisch. Er bezieht sich immer auf die *angestrebten* Auswirkungen und kann daher noch nicht das konkrete Ergebnis meinen. Der identische Wortlaut der Informationspflicht über die Logik und die Auswirkungen deutet daraufhin, dass die Informationspflichten immer gleichlaufen. Das sieht auch die Art. 29-Datenschutzgruppe in ihren Leitlinien zu automatisierten Entscheidungen genauso.[51]

Die Informationspflichten über die Logik und die angestrebten Auswirkungen beziehen sich damit auf den Zeitpunkt vor der eigentlichen Verarbeitung, sodass sie *ex ante* vor allem „die abstrakte Funktionalität der Datenverarbeitung"[52] umfassen.

III. Inhalt der Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO

1. Aussagekräftige Informationen über die involvierte Logik

a) Involvierte Logik

Die involvierte Logik umfasst die Methoden und Kriterien der Datenverarbeitung, d. h. etwa die Funktionsweise eines genutzten

---

[49] S. zum Umfang des Auskunftsrechts nach Art. 15 DSGVO: Kapitel 7 C.I. (S. 261).

[50] *Knitter*, Digitale Weisungen, 2022, S. 172; *Kumkar/Roth-Isigkeit*, JZ 2020, 277-286, 283 ff.; a. A. *Köhnlechner*, DSRITB 2018, 173, 174.

[51] *Art. 29-Datenschutzgruppe*, WP251rev.01, S. 17.

[52] *Knitter*, Digitale Weisungen, 2022, S. 172; *Martini*, Blackbox Algorithmus, 2018, S. 192; *Kumkar/Roth-Isigkeit*, JZ 2020, 277-286, 283 ff.

Algorithmus.[53] Die konkrete Formel muss aber nicht offengelegt werden.[54] So können auch Geschäftsgeheimnisse und Urheberrechte an der Software gewahrt werden.[55] Erwägungsgrund 63 S. 5 DSGVO normiert ausdrücklich, dass diese Rechte nicht beeinträchtigt werden sollen. Das hat auch der BGH zum Scoring der SCHUFA entschieden[56]: In dem Urteil hat sich der BGH mit der Reichweite des Auskunftsanspruchs aus § 34 Abs. 4 S. 1 Nr. 4 BDSG a. F befasst. Nach dieser Vorschrift soll eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittelung erhebt, speichert oder verändert, der betroffenen Person über „das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form" Auskunft erteilen. Der BGH hat entschieden, dass die *Score*-Formel nicht offengelegt werden muss. Ein transparentes Verfahren werde für die betroffene Person vielmehr dadurch erreicht, „dass für [die Betroffene] ersichtlich ist, welche konkreten Umstände als Berechnungsgrundlage in der Ermittlung des Wahrscheinlichkeitswerts eingeflossen sind" [57] . Die abstrakten Vergleichsgruppen und Gewichtungen müssten nicht offengelegt werden, vielmehr reiche es aus, wenn die eingeflossenen Daten und der „Umstand ihres Einflusses" auf das konkrete Berechnungsergebnis zu offenbaren sind.[58] Bei Art. 13 Abs. 2 lit. f sowie 14 Abs. 2 lit. g DSGVO kann sich die Information aber noch nicht auf das konkrete Berechnungsergebnis beziehen, weil letzteres noch nicht vorliegt.

Bei maschinell lernenden Systemen hilft es aber auch nicht zwingend weiter, wenn man die Funktionsweise des Algorithmus erklärt: Ein solches System wird ständig weiterentwickelt. [59] Weder das Wissen über den Ausgangsalgorithmus noch die Kenntnis der Trainingsdaten helfen der betroffenen Person weiter, den (abstrakten) Entscheidungsvorgang zu

---

[53] Kühling/Buchner/*Bäcker*, Art. 13 DSGVO Rn. 54.

[54] Paal/Pauly/*Paal/Hennemann*, Art. 13 DSGVO Rn. 31b m. w. N.; *Gausling*, ZD 2019, 335, 340; *Hoeren/Niehoff*, RW 2018, 47, 56 f.; *Lorenz*, VuR 2019, 213, 219; *Sesing*, MMR 2021, 288, 292.

[55] *Gausling*, ZD 2019, 335, 340 f.

[56] BGH, 28.1.2014 – VI ZR 156/13, NJW 2014, 1235.

[57] BGH, 28.1.2014 – VI ZR 156/13, NJW 2014, 1235, 1237 Rn. 29.

[58] BGH, 28.1.2014 – VI ZR 156/13, NJW 2014, 1235, 1237 Rn. 29.

[59] *Hoeren/Niehoff*, RW 2018, 47, 58.

verstehen.[60] Bei derartigen Systemen können Ansätze von XAI helfen, die Entscheidung nachträglich zu verstehen.[61] Im Hinblick auf die vorgelagerte Erklärung der involvierten Logik muss der betroffenen Person bei maschinell lernenden Systemen dargelegt werden, wie das System grundsätzlich funktioniert und welche Parameter bei einer künftigen Entscheidung berücksichtigt werden.[62] Die konkrete Formel des Algorithmus muss aber nicht offengelegt werden.

b) Aussagekräftige Informationen

Die Informationen über die involvierte Logik müssen *aussagekräftig* sein. Hilfreich bei der Auslegung des Merkmals ist die englische Sprachfassung der DSGVO, in der es *meaningful information* heißt.[63] Der englische Begriff *meaningful* (dt. „bedeutsam") geht über den deutschen Begriff der Aussagekraft hinaus. Gemeint ist damit, dass die betroffene Person anhand der Informationen in die Lage versetzt werden soll, „Rückschlüsse zu den wesentlichen Bedeutungszusammenhängen ziehen zu können"[64]. Die Verantwortliche muss daher die involvierte Logik in einer Form darstellen, dass die betroffene Person die Informationen auf die bevorstehende Verarbeitung übertragen kann. Die Informationen dürfen nicht derart abstrakt sein, dass sie für sich genommen keinen Aussagewert mehr für die konkrete Situation haben.[65]

Aussagekräftig sind die Informationen zudem auch dann, wenn sie in einer für die betroffenen Person verständlichen Art und Weise präsentiert werden.[66]

---

[60] *Dies.*, RW 2018, 47, 58.

[61] S. dazu bereits: Kapitel 4 A.II. (S. 42); zu einem Recht auf Begründung s. Kapitel 7 B.V.3 (S. 259); Kapitel 11 F. (S. 386).

[62] So auch: *Heine*, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis, 2023, S. 347; *Knitter*, Digitale Weisungen, 2022, S. 177;

[63] *Kumkar/Roth-Isigkeit*, JZ 2020, 277-286, 284 ff.

[64] *Dies.*, JZ 2020, 277-286, 284 ff.

[65] Vgl. *Martini*, Blackbox Algorithmus, 2018, S. 181.

[66] *Kumkar/Roth-Isigkeit*, JZ 2020, 277, 284 ff.

Damit bezieht sich das Erfordernis auch auf die Vorgaben des Art. 12 DSGVO.[67]

2. Tragweite und Auswirkungen der Verarbeitung

Die Verantwortliche muss die betroffene Person ebenfalls über die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person informieren. Die betroffene Person muss wissen, welche Entscheidungsmöglichkeiten bestehen und zu welchen Ergebnissen sie führen könnten.[68] Dabei muss die betroffene Person in der Lage sein, die Auswirkungen einordnen und einschätzen zu können.[69] Die möglichen Auswirkungen der Verarbeitung hängen auch davon ab, *welche* Daten verarbeitet werden und *wie* sie verarbeitet werden: Handelt es sich um „einfache" personenbezogene Daten oder sensible Daten nach Art. 9 DSGVO? Werden geeignete Schutzmaßnahmen für die Daten getroffen, d. h. werden sie anonymisiert oder pseudonymisiert?[70] All diese Informationen benötigt die betroffene Person, um die Tragweite und Auswirkung der Verarbeitung zu begreifen.

IV. Umsetzung der Informationspflichten in der Praxis

1. Ausgangsproblem: Schriftliche Erklärungen und Komplexität

Die Informationspflichten dürfen die betroffene Person nicht überfordern. Häufig werden Informationen wie etwa AGB oder Datenschutzerklärungen der betroffenen Person in schriftlicher Form und in erheblichem Umfang zur Verfügung gestellt. Zu umfangreiche Informationen liest die Betroffene im Zweifel nicht, sodass der Zweck der Informationspflicht nicht erfüllt werden würde.[71] Aus einer Umfrage vom 13. Juni 2019 ging etwa hervor, dass von 60 % der Europäerinnen, die Datenschutzerklärungen lesen, nur 13 % die Erklärungen vollständig

---

[67] S. dazu sogleich unter: Kapitel 7 B.IV.2 (S. 254).

[68] Kühling/Buchner/*Bäcker*, Art. 13 DSGVO Rn. 55.

[69] *Ebner*, Weniger ist Mehr?, 2022, S. 205 m. V. a. Plath/*Kamlah*, Art. 13 DSGVO Rn. 29.

[70] S. dazu: Kapitel 6 B.I. (S. 118).

[71] *Martini*, Blackbox Algorithmus, 2018, S. 188; *Sesing*, MMR 2021, 288, 291.

durchlesen.[72] Um es mit *Martinis* Worten zu sagen: „Im schlimmsten Fall verursachen gesetzliche Informationspflichten Unternehmen einen beträchtlichen Bürokratiekostenaufwand, dem kein adäquater Mehrwert für Verbraucher gegenübersteht.“ [73]

Hinzu kommt, dass es bei maschinell lernenden Systemen bereits schwierig ist, überhaupt Vorgänge nachvollziehbar zu erklären.[74] Die Komplexität solcher Systeme erschwert es, die Informationspflichten für die Betroffenen verständlich zu gestalten.

2. Allgemeine Vorgaben des Art. 12 Abs. 1 DSGVO

Art. 12 DSGVO normiert Transparenzvorgaben im Allgemeinen und enthält in Abs. 1 eine „Generalklausel“[75]. Nach Art. 12 Abs. 1 S. 1 DSGVO sollen die Informationen gem. Art. 13, 14 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Das gilt insbesondere für Informationen, die sich speziell an Kinder richten (Art. 12 Abs. 1 S. 1 Hs. 2 DSGVO).

Möglich ist es auch, die Informationen mündlich zu erteilen (Art. 12 Abs. 1 S. 3 DSGVO). Das ist aber bei der Datenverarbeitung mittels algorithmischer Systeme, die im Bewerbungsverfahren oder bestehenden Arbeitsverhältnis eingesetzt werden, angesichts des Umfangs und der Tragweite der Verarbeitung nicht empfehlenswert und wird daher nicht näher untersucht.

a) Präzise und transparente Form

Telos der Art. 12 ff. DSGVO ist, dass die Verarbeitung nachvollziehbar und erklärbar wird: Die Informationen sollen daher nicht die Verarbeitung umfassend beschreiben, sondern nur die wesentlichen Informationen

---

[72] Pressemitteilung zur Veröffentlichung der Ergebnisse der Eurobarometer-Sonderumfrage zum Thema Datenschutz, 13.06.2019, https://perma.cc/BW8T-BR4T (archiviert am 01.12.2022); umfassend dazu s. *Ebner*, Weniger ist Mehr?, 2022, S. 102 ff.

[73] *Martini*, Blackbox Algorithmus, 2018, S. 189.

[74] S. dazu: Kapitel 4 A.II. (S. 42).

[75] Paal/Pauly/*Paal/Hennemann*, Art. 12 DSGVO Rn. 1.

erhalten, die zur Nachvollziehbarkeit und Erklärbarkeit führen.[76] Präzise und transparent ist daher so zu verstehen, dass die Informationen in knapper Form zur Verfügung gestellt werden müssen.[77] So ähnlich formuliert es auch die Art. 29-Datenschutzgruppe: Eine präzise und transparente Form bedeute, dass die Informationen „auf eine einfache Formel gebracht und griffig formuliert" vorgelegt werden sollten.[78]

b) Verständlichkeit und leichte Zugänglichkeit

Die betroffene Person muss in der Lage sein, die Informationen ohne übermäßigen kognitiven oder zeitlichen Aufwand tatsächlich nachvollziehen zu können.[79] Verständlichkeit bedeutet also auch, eine klare und einfache Sprache zu verwenden und die Art der Information auch vom Zielpublikum abhängig zu machen.[80] Richten sich die Informationen an ein Fachpublikum oder an Kinder? Die Anforderungen an die Verständlichkeit hängen mithin auch von dem Wissen und den kognitiven Fähigkeiten der betroffenen Person ab.[81]

Leicht zugänglich bedeutet, dass die betroffene Person die Information mit den ihr zur Verfügung stehenden (technischen) Mitteln erreichen kann.[82] Bei schriftlichen Mitteilungen müssen diese der betroffenen Person physisch zugänglich sein, bei Informationen auf Websites müssen die Informationen gut sichtbar platziert sein. Sie müssen mit allen gängigen Browsern wiedergegeben werden können und dürfen nicht passwortgeschützt hinter einer Paywall oder hinter Bannern verborgen sein.[83]

---

[76] *Strassemeyer*, DSRITB 2019, 31, 35.

[77] Taeger/Gabel/*Pohle/Spittka*, Art. 12 DSGVO Rn. 10.

[78] *Art. 29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260), S. 7.

[79] Kühling/Buchner/*Bäcker*, Art. 12 DSGVO Rn. 11.

[80] *Art. 29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260), S. 8.

[81] *Dies.*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260), S. 12.

[82] Paal/Pauly/*Paal/Hennemann*, Art. 12 DSGVO Rn. 32; BeckOK Datenschutzrecht/*Quaas*, Art. 12 DSGVO Rn. 16.

[83] Gola/Heckmann/*Franck*, Art. 12 DSGVO Rn. 21.

3. Transparenz durch visuell wahrnehmbare Informationen

Damit die betroffenen Personen die Informationen besser aufnehmen können, sollen die Informationen visuell wahrnehmbar aufbereitet werden.[84] Die visuell wahrnehmbaren Informationen können unterstützend zu schriftlichen Informationen verwendet werden.

a) Bildsymbole

Nach Art. 12 Abs. 7 DSGVO können die Informationen in Kombination mit standardisierten Bildsymbolen bereitgestellt werden. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie gem. Art. 12 Abs. 7 S. 2 DSGVO maschinenlesbar sein. Nach Art. 12 Abs. 8 DSGVO kann die EU-Kommission gem. Art. 92 DSGVO delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole erlassen. Diese Befugnis hat die EU-Kommission noch nicht umgesetzt. Die Symbole sollten hinreichend groß und aussagekräftig ausgestaltet sein: Die betroffene Person muss erkennen, wie die Daten verarbeitet wurden und welche Ergebnisse des algorithmischen Systems als Grundlage für die Entscheidung gewählt wurden.[85]

b) Ablaufdiagramme

Ablaufdiagramme stellen grafisch einen Ablauf einer Entscheidung bzw. eines Prozesses dar.[86] Die Diagramme können animiert dargestellt werden, damit der betroffenen Person in einem Video die relevanten Informationen präsentiert werden können.[87] Durch animierte Abläufe können kognitive Reize stimuliert und so die Auffassung der Betroffenen gesteigert werden.[88]

---

[84] *Conrad*, DSRITB 2019, 391, 403 f.; *Ebner*, Weniger ist Mehr?, 2022, S. 117.
[85] *Martini*, Blackbox Algorithmus, 2018, S. 189.
[86] *Strassemeyer*, DSRITB 2019, 31, 42; *Ebner*, Weniger ist Mehr?, 2022, S. 117.
[87] *Strassemeyer*, DSRITB 2019, 31, 43.
[88] *Ders.*, DSRITB 2019, 31, 43.

c) Gamification

Unter *Gamification* meint, dass Spielelemente, -designs und -mechanismen in einem spielfremden Kontext eingesetzt werden. [89] Baut man etwa Spielelemente in ein Ablaufdiagramm mit ein, wird die betroffene Person aktiv angesprochen. *Strassemeyer* schlägt vor, dass Mobileapps eingesetzt werden, die den Verarbeitungsumfang videografisch vermitteln und die Nutzerin interaktiv einbinden.[90] Dadurch wird die Bereitschaft erhöht, dass man sich mit der Datenverarbeitung tatsächlich inhaltlich auseinandersetzt.[91]

V. Informations-/Erklärungspflichten *de lege ferenda*

Die Ausführungen zeigen, dass die Informationspflichten *de lege lata* noch nicht ausreichen, dass die Entscheidung, bei der ein maschinell lernendes System entscheidungsunterstützend eingesetzt wird, hinreichend transparent ist: Aussagekräftige Informationen über die involvierte Logik muss die Verantwortliche nur bereitstellen, wenn es sich um eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung handelt. Bildsymbole können, müssen aber nicht verwendet werden. Die Informationspflicht bezieht sich zudem nicht auf eine Erklärung oder gar Begründung *ex post*, also nach der Verarbeitung der personenbezogenen Daten. Daher folgen nun drei Vorschläge, wie man die Informationspflichten *de lege ferenda* ausgestalten könnte.

1. Informationspflichten auch bei teilautomatisierten Entscheidungen

Die Verantwortliche ist nicht verpflichtet, über die verwendete Logik bei teilautomatisierten Entscheidungen zu informieren. [92] Eine Informationspflicht in Bezug auf die Logik, Tragweite und die angestrebten Auswirkungen der Verarbeitung bei algorithmischen Systemen im Arbeitsrecht, wie etwa der Bewerberinnen(vor-)auswahl, besteht somit nicht.

---

[89] *Ders.*, DSRITB 2019, 31, 43.
[90] *Ders.*, DSRITB 2019, 31, 44.
[91] *Ders.*, DSRITB 2019, 31, 44.
[92] S. dazu: Kapitel 7 B.I. (S. 248).

Es ist aber in bestimmten Fällen notwendig, dass eine Informationspflicht über die eingesetzte Logik auch bei maschinell lernenden Systemen besteht, die bloß entscheidungsunterstützend eingesetzt werden.[93] Solche Fälle liegen vor, wenn die maschinell lernenden Systeme in grundrechtssensitiven Bereichen, wie etwa bei der Personalauswahl, eingesetzt werden.[94] Wie bereits herausgearbeitet worden ist, kann sich der Einsatz algorithmischer Systeme erheblich auf die menschliche Entscheidung auswirken, wenn diese unterstützend eingesetzt werden.[95] Auch bei bloß entscheidungsunterstützenden Systemen werden die Grundrechte der betroffenen Person gefährdet.[96]

2. Pflicht zur Verwendung visueller Techniken

Zu kritisieren ist zudem, dass Art. 12 Abs. 7 DSGVO bislang nur als „Kann-Vorschrift" ausgestaltet ist. Damit die Unternehmen und Verantwortlichen der Datenverarbeitung aber Bildsymbole verwenden, müsste die Vorschrift als gesetzliche Pflicht ausgestaltet werden. Schließlich kann man auch über die Pflicht, die Informationen interaktiv auszugestalten, nachdenken. Zwar erfordert es weit mehr Ressourcen, die Informationspflichten auch visuell wahrnehmbar auszugestalten. Am Ende wird aber das Vertrauen durch leichter zugängliche Informationen steigen, sodass es sich für die Verantwortlichen lohnt, in eine möglichst ansprechende Art der Informationsvermittlung zu investieren. Ohne eine rechtliche Pflicht besteht aber kein Handlungszwang für die Verantwortliche, solche Techniken zu verwenden.

---

[93] Vgl. *Lorentz*, Profiling – Persönlichkeitsschutz durch Datenschutz?, 2020, S. 237; *Martini*, Blackbox Algorithmus, 2018, S. 178; *Schwarze*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 8 Rn. 32, der der Ansicht ist, den Auskunftsanspruch gem. Art. 13 Abs. 2 lit. f DSGVO richtigerweise auf den Einsatz automatisierter Entscheidungsfindung zur Vorbereitung einer Entscheidung der Arbeitgeberin zu erstrecken.

[94] Vgl. *Martini*, Blackbox Algorithmus, 2018, S. 178; *Sesing*, MMR 2021, 288, 290.

[95] S. dazu: Kapitel 6 D.IV.3.b) (S. 216).

[96] Vgl. zur Ausweitung der Informationspflicht *Art. 29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259), S. 27.

3. Recht auf Begründung der Entscheidung als Lösung?

Wie ausgeführt worden ist, ist die Informationspflicht über die involvierte Logik und die angestrebte Verarbeitung beschränkt auf den *abstrakten* Verarbeitungsvorgang und nicht auf die *konkrete* Entscheidung.[97]

Wischmeyer schlägt deshalb vor, über ein Recht auf Begründung der Entscheidung nachzudenken, um die individuelle Nachvollziehbarkeit der Entscheidung zu sichern.[98] Beispielsweise gibt es im Verwaltungsrecht eine Begründungspflicht bei Verwaltungsakten (§ 39 Abs. 1 VwVfG), die nur bei normierten Ausnahmen nach § 39 Abs. 2 VwVfG nicht greift. In der DSGVO ist eine Begründungspflicht nicht normiert. Lediglich Erwägungsgrund 71 S. 4 DSGVO erwähnt bei ausschließlich automatisierten Entscheidungen ein Recht auf „Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung". Allerdings wurde dieses Recht in Art. 22 Abs. 3 DSGVO nicht übernommen.[99] Selbst wenn man das Recht aus den Erwägungsgründen herleitet, umfasst ein Recht auf Erläuterung nicht zwingend ein Recht auf Begründung. Erläutern meint zunächst, den Inhalt der Entscheidung zu erklären.[100]

Eine pauschale Pflicht zur Begründung einer Entscheidung, die unterstützend mit maschinell lernenden Systemen getroffen wurde, greift in die allgemeine Handlungsfreiheit gem. Art. 2 Abs. 1 GG ein.[101] Auf unionaler Ebene wird die allgemeine Handlungsfreiheit jedenfalls auf unternehmerischer Ebene durch Art. 16 GRCh geschützt.[102]

Grundsätzlich muss man im Privatrechtsverhältnis keine Entscheidung begründen. *Martini* führt daher zutreffend aus, dass auch bei

---

[97] Kapitel 7 B.III.1. (S. 250).

[98] *Wischmeyer*, AöR 143 (2018), 1, 55; dazu auch: *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018, S. 45; *Martini*, Blackbox Algorithmus, 2018, S. 190; *Klar*, BB 2019, 2243, 2251; kritisch dazu: *Kumkar/Roth-Isigkeit*, JZ 2020, 277-286, 286 ff.

[99] S. Kapitel 6 D.IV.6. (S. 232).

[100] *Martini*, Blackbox Algorithmus, 2018, S. 191.

[101] *Ders.*, Blackbox Algorithmus, 2018, S. 344.

[102] Vgl. Calliess/Ruffert/*Ruffert*, Art. 16 GRCh Rn. 2.

algorithmenbasierten Entscheidungen keine pauschale Begründungspflicht gelten könne. Die Begründungspflicht lasse sich nur bei grundrechtssensiblen Bereichen rechtfertigen: Algorithmische Entscheidungen haben anders als menschliche Entscheidungen kein tieferes Verständnis für die Entscheidung, sie treffen die Entscheidung korrelativ und können daher ungeahnte „Fehler" machen. [103] Das rechtfertige eine besondere Begründungspflicht bei grundrechtssensiblen Bereichen.[104]

Eine Begründungspflicht wird aber je nach Art des maschinell lernenden Systems auch technisch schwierig. Bei maschinell lernenden Systemen, bei denen etwa ein neuronales Netz eingesetzt wird, wissen die Entwicklerinnen häufig selbst nicht, wie genau eine Entscheidung zustande gekommen ist.[105] Helfen können Ansätze von XAI. [106] Mithilfe von LRP kann der Entscheidungsprozess eines neuronalen Netzes rückwärts abgespielt werden. Eine sog. *Heatmap* ermöglicht es, positive und negative Entscheidung der *Hidden Layer* sichtbar zu machen.[107]

Die betroffenen Personen werden bereits nach den Informationspflichten gem. Art. 13 Abs. 2 lit. f DSGVO sowie Art. 14 Abs. 2 lit. g DSGVO über die Funktionsweise des Algorithmus und die zugrundeliegenden Parameter informiert.[108] Wird das Ergebnis begründet, werden der Person noch konkrete Informationen im Hinblick auf die individuelle Entscheidung mitgeteilt. Insofern muss die Person über die Vergleichsgruppe und die individuellen Besonderheiten, die zur Entscheidung geführt haben, informiert werden.[109] Eine Grenze besteht dann, wenn Rechte Dritter entgegenstehen. [110] Solche Rechte können insbesondere Geschäftsgeheimnisse oder sonstige überwiegende legitime Interessen Dritter sein.[111]

---

[103] *Martini*, Blackbox Algorithmus, 2018, S. 344.
[104] *Ders.*, Blackbox Algorithmus, 2018, S. 344.
[105] S. dazu: Kapitel 4 (S. 39).
[106] S. Kapitel 4 A.II. (S. 42).
[107] S. dazu: Kapitel 4 A.II. (S. 42).
[108] Kapitel 7 B.III.1. (S. 250).
[109] *Martini*, Blackbox Algorithmus, 2018, S. 197.
[110] *Ders.*, Blackbox Algorithmus, 2018, S. 197.
[111] *Ders.*, Blackbox Algorithmus, 2018, S. 197.

Ein Recht auf Begründung der Entscheidung kann daher – je nach technischer und rechtlicher Möglichkeit – eine Lösung sein, um mehr Transparenz[112] bezüglich der Entscheidung für die betroffene Person zu erreichen.

In der künftigen KI-VO wird jedenfalls ein Recht auf Erklärung der individuellen Entscheidungsfindung verankert sein: Art. 68c KI-VO-PARL sieht ein solches Recht vor.[113]

C. Rechte der betroffenen Person

Der betroffenen Person stehen nach Art. 15 DSGVO bis Art. 21 DSGVO verschiedene Rechte zu, die im Hinblick auf den Einsatz algorithmischer Systeme relevant werden können. Untersucht werden im Folgenden das Auskunftsrecht nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO und das Recht auf Löschung gem. Art. 17 DSGVO. Art. 15 und Art. 17 DSGVO sind vor allem in der Praxis besonders relevant.[114]

I. Auskunftsrecht gem. Art. 15 DSGVO

Rund um das Auskunftsrecht nach Art. 15 DSGVO ist vieles umstritten und unklar.[115] Im Folgenden wird insbesondere darauf eingegangen, ob das Auskunftsrecht auch die Auskunft über die *Output*-Daten umfasst.[116]

1. Zweistufiges Auskunftsrecht

Art. 15 Abs. 1 DSGVO gewährt der betroffenen Person Recht auf Auskunft über die verarbeiteten, sie betreffenden personenbezogenen Daten.

---

[112] Kapitel 4 B.I. (S. 45).

[113] S. dazu: Kapitel 11 F. (S. 386).

[114] *Gausling*, in: Ballestrem/Bär/Gausling u.a. (Hrsg.), Künstliche Intelligenz, 2020, S. 11, 44.

[115] *Eickstädt/Weaver*, DSRITB 2020, 287; *Maschmann*, NZA-Beilage 2022, 50-56; *Korch/Chatard*, ZD 2022, 482; *Paal/Kritzer*, NJW 2022, 2433-2439.

[116] S. dazu sogleich unter: Kapitel 7 C.I.2. (S. 262).

Das Auskunftsrecht ist zweistufig ausgeprägt: Auf der ersten Stufe hat die betroffene Person das Recht, Auskunft darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet wurden.[117] Ist das nicht der Fall, muss der Betroffenen diese Information mitgeteilt werden.[118]

Werden sie betreffende personenbezogene Daten verarbeitet, hat die betroffene Person auf der zweiten Stuft das Recht auf Auskunft, welche Daten verarbeitet werden, sowie das Recht auf weitere Informationen, die in Art. 15 Abs. 1 lit. a - h DSGVO aufgeführt sind.[119] Die betroffene Person hat demnach unter anderem das Recht auf Auskunft über die Verarbeitungszwecke, über die Kategorien verarbeiteter personenbezogener Daten, über die Empfängerinnen oder Kategorien von Empfängerinnen, gegenüber denen die personenbezogenen Daten offengelegt worden sind.

2. Umfang des Auskunftsrechts: Auskunft über die Output-Daten

Das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO bezieht sich auf die Information über die verarbeiteten Daten der betroffenen Person. Regelmäßig wird die betroffene Person ein Interesse daran haben, auch über das Ergebnis der Verarbeitung informiert zu werden, d. h. über die neu generierten *Output*-Daten. Fraglich ist allerdings, ob man der Betroffenen nach der Verarbeitung gem. Art. 15 Abs. 1 DSGVO Informationen über die *Output*-Daten bereitstellen muss.[120]

Der Wortlaut des Art. 15 Abs. 1 DSGVO sieht eine Auskunft über das Ergebnis nicht vor. Im Rahmen der automatisierten Entscheidungsfindung besteht nach Art. 15 Abs. 1 lit. h DSGVO ein Recht auf Auskunft über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. Auch hier sieht der Wortlaut nicht explizit vor, dass die betroffene Person über das Ergebnis in Kenntnis zu setzen ist. Einige Stimmen in der Literatur sprechen sich dafür aus, dass die Verantwortliche im Rahmen von Art. 15 Abs. 2 lit. h DSGVO

---

[117] Paal/Pauly/*Paal*, Art. 15 DSGVO Rn. 19.
[118] Paal/Pauly/*ders.*, Art. 15 DSGVO Rn. 19.
[119] Paal/Pauly/*ders.*, Art.15 DSGVO Rn. 20.
[120] *Hacker*, NJW 2020, 2142, 2144; *Martini*, Blackbox Algorithmus, 2018, S. 198 ff.

die Auswertungsergebnisse und die Entscheidungen mitteilen muss. [121] *Krügel/Pfeiffenbring* lehnen die Pflicht zur Begründung der Entscheidung ab:[122] Eine Begründungspflicht gehe über das hinaus, was die Rechtsordnung bei einer menschlichen Entscheidung verlange. Die Beweggründe einer menschlichen Entscheidung blieben stets im Verborgenen. Erwägungsgrund 63 S. 2 DSGVO sieht hingegen vom Auskunftsanspruch auch die „Untersuchungsergebnisse" erfasst. Zwar bezieht sich Erwägungsgrund 63 S. 2 DSGVO nur auf gesundheitsbezogene Daten. Man könnte Erwägungsgrund 63 S. 2 DSGVO jedoch auch so deuten, dass der Unionsgesetzgeber insgesamt ein transparentes Ergebnisprotokoll bezweckt und somit die Ergebnisse der Verarbeitung stets vom Auskunftsanspruch erfasst sind. [123] Die Erwähnung des „Untersuchungsergebnisses" in Erwägungsgrund 63 S. 2 DSGVO zeigt aber, dass der Verordnungsgeber das Ergebnis nicht versehentlich „vergessen" hat. Vielmehr hat er eine bewusste Entscheidung gegen die Auskunft über das Verarbeitungsergebnis und dessen Erklärung getroffen, indem er in Art. 15 Abs. 1 DSGVO ganz genau die Informationen, über die eine Auskunft erteilt wird, aufgelistet hat. Wie bereits ausgeführt, ist der Inhalt der Auskunftsrechte über die involvierte Logik und die Tragweite der angestrebten Verarbeitung sowohl in Art. 13 Abs. 2 lit. f DSGVO als auch in Art. 14 Abs. 2 lit. g DSGVO und Art. 15 Abs. 1 lit. h DSGVO gleich.[124]

Auch im Falle der automatisierten Entscheidungsfindung sprechen somit die überzeugenderen Argumente dafür, dass die Pflicht zur Begründung der Entscheidung nicht vom Auskunftsrecht erfasst ist. Das Auskunftsrecht

---

[121] Kühling/Buchner/*Bäcker*, Art. 15 DSGVO Rn. 27; Gola/Heckmann/*Franck*, Art. 15 DSGVO Rn. 19; so auch: *Lorentz*, Profiling – Persönlichkeitsschutz durch Datenschutz?, 2020, S. 249; *Wieder*, DSRITB 2018, 505, 515.

[122] *Krügel/Pfeiffenbring*, in: Ebers/Heinze/Krügel u.a. (Hrsg.), Künstliche Intelligenz und Robotik, 2020, § 11 Rn. 77.

[123] Vgl. *Martini*, Blackbox Algorithmus, 2018, S. 200.

[124] Kapitel 7 B.II. (S. 249).

bezieht sich somit auf Informationen über das Entscheidungsverfahren, nicht aber auf die Begründung und genaue Erklärung der Ergebnisse.[125]

Die Risiken automatisierter Entscheidungen betreffen das allgemeine Persönlichkeitsrecht der betroffenen Person, wenn Personen in automatisierten Entscheidungen zu „reinen Objekten mathematisch-probabilistischer Berechnungen [gemacht] werden“[126]. Selbst wenn man davon ausgeht, dass das Auskunftsrecht nach Art. 15 Abs. 1 lit. h DSGVO auch die Begründungspflicht sowie das konkrete Ergebnis umfasst, wird das allgemeine Persönlichkeitsrecht dadurch nicht geschützt. Um systematische *bias*, fehlerhafte Konzeptannahmen oder Einzelgewichtungen von Entscheidungsfaktoren zu erkennen, müsste man das maschinell lernende System in seiner Gesamtheit auswerten. Eine reine Einzelfallbetrachtung reiche nicht aus.[127] Ein Recht auf Begründung könnte aber – wie soeben ausgeführt – auch die tragenden Gründe im Vergleich zu den anderen Personen aufzeigen.[128]

II. Recht auf Berichtigung gem. Art. 16 DSGVO

Nach Art. 16 S. 1 DSGVO ist die betroffene Person berechtigt, von der Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

Wann ein Datum „unrichtig“ ist, wird in der DSGVO nicht erläutert. Nach dem BVerwG sind Daten unrichtig, wenn die enthaltenen Informationen nicht mit der Realität übereinstimmen.[129] Diese Auslegung legt auch die

---

[125] *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018, S. 31; *Martini*, Blackbox Algorithmus, 2018, S. 191; a. A. *Lorentz*, Profiling – Persönlichkeitsschutz durch Datenschutz?, 2020, S. 249.

[126] *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018, S. 31.

[127] *Dies.*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018, S. 31; i. E. auch: *Wischmeyer*, AöR 143 (2018), 1, 54.

[128] Kapitel 7 C.I.2. (S. 262).

[129] BVerwG, 4.3.2004 – 1 WB 32/03, NVwZ 2004, 626, Rn. 11.

Literatur bei Art. 16 DSGVO zugrunde[130], wenngleich der Begriff „unrichtig" unionsrechtlich autonom bestimmt werden muss.[131] Nur Tatsachen können objektiv richtig oder unrichtig sein, da sie einem Beweis zugänglich sind.[132] Werden algorithmische Systeme bei der Personalauswahl eingesetzt, kann es zu einer falschen Einordnung von Personen kommen, wenn die *Input-Daten*, d. h. die personenbezogenen Daten, auf denen ein Profil basiert, fehlerhaft sind.[133] Auch geschätzte Daten, die nicht entsprechend gekennzeichnet sind, können unrichtig sein, wenn der Eindruck erweckt wird, es handele sich um Tatsachen.[134] Nicht vom Berichtigungsanspruch erfasst sind Werturteile, die etwa die Verantwortliche auf Grundlage der Entscheidung des algorithmischen Systems formuliert hat.[135] Die Entscheidungen sind als Werturteile nicht den Kategorien „falsch" oder „richtig" zugänglich.[136] Hält die Arbeitgeberin basierend auf der Einschätzung des algorithmischen Systems und auf ihrem eigenen Eindruck von der Bewerberin diese für nicht geeignet für die vakante Position, ist dieses Werturteil nicht dem Berichtigungsanspruch nach Art. 16 S. 1 DSGVO zugänglich.

Wie bedeutsam oder wie groß der Umfang der unrichtigen Daten ist, darauf kommt es nicht an: Auch kleinere Unrichtigkeiten sind relevant, soweit Grundrechtspositionen der betroffenen Person beeinträchtigt werden.[137] Bloße Grammatikfehler o. Ä. ohne eigenen Aussagegehalt sind hingegen irrelevant.[138]

---

[130] Ehmann/Selmayr/*Kamann/Braun*, Art. 16 DSGVO Rn. 14; Gola/Heckmann/*Reif*, Art. 16 DSGVO Rn. 13; Kühling/Buchner/*Herbst*, Art. 16 DSGVO Rn. 8.

[131] Ehmann/Selmayr/*Kamann/Braun*, Art. 16 DSGVO Rn. 13.

[132] Kühling/Buchner/*Herbst*, Art. 16 DSGVO Rn. 8.

[133] Ehmann/Selmayr/*Kamann/Braun*, Art. 16 DSGVO Rn. 14.

[134] Ehmann/Selmayr/*dies.*, Art. 16 DSGVO Rn. 14.

[135] *Martini*, Blackbox Algorithmus, 2018, S. 202.

[136] *Ders.*, Blackbox Algorithmus, 2018, S. 202; Paal/Pauly/*Paal*, Art. 16 DSGVO Rn. 15; Kühling/Buchner/*Herbst*, Art. 16 DSGVO Rn. 8 f.; a. A. Ehmann/Selmayr/*Kamann/Braun*, Art. 16 DSGVO Rn. 21.

[137] Ehmann/Selmayr/*Kamann/Braun*, Art. 16 DSGVO Rn. 16.

[138] BeckOK Datenschutzrecht/*Worms*, Art. 16 DSGVO Rn. 52; Ehmann/Selmayr/*Kamann/Braun*, Art. 16 DSGVO Rn. 16.

Bei algorithmischen Systemen, die zur Personalauswahl eingesetzt werden, ist der Berichtigungsanspruch somit vor allem im Hinblick auf die verarbeiteten Ausgangsdaten relevant.[139] Die betroffene Person hat gem. Art. 15 Abs. 1 DSGVO[140] ein Recht auf Auskunft über die verarbeiteten personenbezogenen Daten und kann erkennen, ob die Daten, die verarbeitet wurden, richtig waren.

Nach Art. 16 S. 2 DSGVO kann die betroffene Person die Vervollständigung unvollständiger personenbezogener Daten verlangen. Nicht jeder unvollständige Datensatz löst einen Vervollständigungsanspruch nach Art. 16 S. 2 DSGVO aus.[141] Vielmehr muss im Hinblick auf den Zweck der Verarbeitung überprüft werden, welches Risiko die unvollständige Verarbeitung für die Betroffene birgt.[142] Sind die Informationen, die für eine neu zu besetzende Stelle relevant sind, nur vereinzelt von der betroffenen Person verfügbar, besteht das Risiko, dass das algorithmische System zu einem unrichtigen Ergebnis gelangt.[143] In einem solchen Fall wären die Daten als unvollständig i. S. v. Art. 16 S. 2 DSGVO anzusehen.[144] Die fehlenden Daten müssen nachträglich in den Datensatz aufgenommen werden.

Berichtigungs- und Vervollständigungsanspruch sind unverzüglich zu erfüllen.[145]

III. Recht auf Löschung gem. Art. 17 DSGVO

Nach Art. 17 Abs. 1 DSGVO kann die betroffene Person von der Verantwortlichen verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Unter bestimmten in Art. 17 lit. a-f DSGVO genannten Gründen ist die Verantwortliche dazu verpflichtet, personenbezogene Daten unverzüglich zu löschen. Für den

---

[139] *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018, S. 266.

[140] Kapitel 7 C.I. (S. 261).

[141] BeckOK Datenschutzrecht/ *Worms*, Art. 16 DSGVO Rn. 18.

[142] BeckOK Datenschutzrecht/*ders.*, Art. 16 DSGVO Rn. 58.

[143] Vgl. *Lorentz*, Profiling – Persönlichkeitsschutz durch Datenschutz?, 2020, S. 251.

[144] BeckOK Datenschutzrecht/ *Worms*, Vgl. Art. 16 DSGVO Rn. 59.

[145] BeckOK Datenschutzrecht/*ders.*, Art. 16 DSGVO Rn. 62.

Untersuchungsgegenstand werden vor allem Art. 17 Abs. 1 lit. a und b DSGVO als Löschgründe einschlägig sein.

Art. 17 Abs. 2 DSGVO ist einschlägig, wenn die Verantwortliche die personenbezogenen Daten öffentlich gemacht hat und sie gem. Art. 17 Abs. 1 DSGVO zur Löschung verpflichtet ist. Die Vorschrift ist bei algorithmischen Systemen, die im Bewerbungsverfahren oder bestehenden Arbeitsverhältnis eingesetzt werden, nicht relevant, weil die personenbezogenen Daten nicht öffentlich gemacht werden.

Die Absätze 1 und 2 gelten nicht, wenn die Verarbeitung nach Art. 17 Abs. 3 lit. a-e DSGVO erforderlich ist. Das ist z. B. der Fall, wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist (lit. a). Für den Untersuchungsgegenstand ist keine Ausnahme nach Abs. 3 einschlägig.

1. Daten sind für Erhebungs- und Verarbeitungszwecke nicht mehr erforderlich (Art. 17 Abs. 1 lit. a DSGVO)

Die Verantwortliche ist nach Art. 17 Abs. 1 lit. a DSGVO verpflichtet, die Daten zu löschen[146], wenn sie für die Zwecke der Datenverarbeitung nicht mehr notwendig sind.

Daten abgelehnter Bewerberinnen müssen somit gelöscht werden. [147] Gleichwohl können die Daten jedoch für maschinell lernende Systeme relevant sein: Anhand vergangenheitsbezogener Daten kann ein derartiges System weiter trainiert werden, um sie auf neue Bewerberinnen anzuwenden. [148] An dieser Stelle wird auf den Abschnitt zum Training maschinell lernender Systeme verwiesen.[149]

---

[146] Vgl. zu einem DSGVO-Löschvorgang etwa: *Knuchel/Ebert*, DuD 2020, 126.

[147] Paal/Pauly/*Paal*, Art. 17 DSGVO Rn. 23.

[148] Vgl. etwa *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018, S. 220.

[149] Kapitel 6 B. (S. 117).

2. Betroffene Person widerruft ihre Einwilligung (Art. 17 Abs. 1 lit. b DSGVO)

Die personenbezogenen Daten müssen gelöscht werden, wenn die betroffene Person ihre Einwilligung widerruft. Der Widerruf wirkt *ex nunc*, d. h., die Verarbeitung der Daten auf Grundlage der Einwilligung bis zum Widerruf bleibt rechtmäßig.[150] Fraglich ist, ob bereits trainierte maschinell lernende Systeme weiterverwendet werden dürfen. An dieser Stelle kann auf die Ausführungen im Rahmen der Einwilligung verwiesen werden[151]: Man darf ein solches System nur weiterverwenden, wenn eine Re-Identifikation der (personenbezogenen) Daten ausgeschlossen ist. In diesem Fall kann das Anonymisieren mit dem Löschen gleichgesetzt werden, und es liegt eine wirksame Anonymisierung im Rechtssinne vor. Sind die personenbezogenen Daten anonymisiert, muss es daher möglich sein, das maschinell lernende System trotz des Widerrufs weiterzuverwenden. Andernfalls müssen die Daten aus dem System gelöscht werden. Das kann im Einzelfall auch bedeuten, dass das System nicht mehr verwendet werden darf, wenn die Daten nicht gelöscht werden können.

D. Zwischenergebnis: Erweiterung der Informationspflichten *de lege ferenda*

1. Die Verantwortliche muss bei den untersuchten algorithmischen Systemen eine DSFA gem. Art. 35 Abs. 1 S. 1 DSGVO durchführen.[152] Es gibt jedoch keine Pflicht, die DSFA zu veröffentlichen. Veröffentlicht man die DSFA, ermöglicht man allerdings den betroffenen Personen, sich einen detaillierten Überblick über die Risikobewertung und die geplanten Abhilfemaßnahmen zu verschaffen. Dadurch wird die Datenverarbeitung transparenter und

---

[150] Sydow/Marsch/*Peuker*, Art. 17 DSGVO Rn. 18.
[151] Kapitel 6 B.V.3. (S. 151).
[152] Kapitel 7 A. (S. 241).

das Vertrauen in die Datenverarbeitung mittels algorithmischer Systeme kann wachsen.[153]

2. Nach Art. 13 Abs. 2 lit. f DSGVO, 14 Abs. 2 lit. g DSGVO sowie 15 Abs. 1 lit. h DSGVO hat die betroffene Person das Recht, aussagekräftige Informationen über die involvierte Logik sowie über die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erhalten. *De lege lata* gelten diese Informationspflichten nur für ausschließlich automatisierte Entscheidungen, die gem. Art. 22 Abs. 2 DSGVO unter bestimmten Voraussetzungen ausnahmsweise zulässig sind. [154] Bei grundrechtssensiblen Entscheidungen, also auch bei arbeitsrechtlichen Auswahlentscheidungen, sollten die Pflichten *de lege ferenda* nicht nur auf ausschließlich automatisierte Entscheidungen begrenzt sein. Werden algorithmische Systeme entscheidungsunterstützend eingesetzt, kann das Ergebnis des Systems sich erheblich auf die menschliche Letztentscheidung auswirken. [155] Auch entscheidungsunterstützende Systeme sind für die Grundrechte der betroffenen Person gefährlich, weshalb die betroffene Person über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen der Verarbeitung informiert werden sollte.[156]

3. Die involvierte Logik meint die grundsätzliche Funktionsweise des Algorithmus bzw. Systems sowie die relevanten Parameter.[157] In Bezug auf die Tragweite sowie die Auswirkungen der Verarbeitung muss die Person darüber in Kenntnis gesetzt werden, welche möglichen Konsequenzen die Verarbeitung auf ihre Grundrechte hat und welche Schutzmaßnahmen für ihre personenbezogenen Daten ergriffen werden.[158]

---

[153] Kapitel 7 A.I. (S. 243).
[154] Kapitel 7 B.I. (S. 248).
[155] Kapitel 6 D.IV.3.b) (S. 216).
[156] Kapitel 7 B.V.1. (S. 257).
[157] Kapitel 7 B.III.1.a) (S. 250).
[158] Kapitel 7 B.III.2. (S. 253).

4. Die Informationen müssen gem. Art. 12 Abs. 1 S. 1 DSGVO in präziser und transparenter Form dargestellt sowie verständlich und leicht zugänglich präsentiert werden. Sie müssen daher auf den Empfängerhorizont der betroffenen Person zugeschnitten sein und dürfen keine irrelevanten Informationen enthalten. [159] Es ist nicht verpflichtend, Bildsymbole zu verwenden. *De lege ferenda* sollte es indes eine Pflicht zur Verwendung standardisierter Bildsymbole oder gar auch von Darstellungen per Video geben. [160] Grund dafür ist, dass eine Informationsvermittlung in Textform weniger zugänglich ist und die Gefahr besteht, dass die betroffene Person die Information nicht zur Kenntnis nimmt. Gibt es eine Pflicht zur Verwendung effektiverer alternativer Informationsmittel, wird sichergestellt, dass solche Mittel auch tatsächlich verwendet werden.

5. Ein Recht auf Begründung der Entscheidung ist nach der DSGVO nicht vorgesehen. Es ist aber sinnvoll, ein Recht auf Begründung in bestimmten Fällen einzuführen, um mehr Transparenz für die betroffene Person herzustellen.[161] Die Begründungspflicht kann man – wie *Martini* zutreffend ausführt – nur in grundrechtssensiblen Bereichen rechtfertigen: Maschinell lernende Systeme haben anders als menschliche Entscheidungen kein tiefergehendes Verständnis für die Entscheidung, sie treffen die Entscheidung korrelativ und können ungeahnte „Fehler" machen.[162] Ein Recht auf Begründung ist allerdings mit rechtlichen wie auch mit technischen Hürden verbunden: Zum einen können legitime Interessen Dritter einer Begründung der Entscheidung gegenüberstehen, wie z. B. Geschäftsgeheimnisse. Zum anderen ist es technisch schwierig, den Entscheidungsprozess des Systems offenzulegen. Mithilfe von XAI ist es aber – jedenfalls in Teilen

---

[159] Kapitel 7 B.IV.2. (S. 254).

[160] Kapitel 7 B.V.2. (S. 258).

[161] Kapitel 7 B.V.3. (S. 259); s. zum Recht auf Begründung nach Art. 68c KI-VO-PARL: Kapitel 11 F. (S. 386).

[162] Kapitel 3 C. (S. 36).

– heutzutage möglich, bestimmte Entscheidungsprozesse offenzulegen.[163]

[163] Kapitel 4 A.II. (S. 42).

Teil 2

Zusammenfassung

1. Werden personenbezogene Daten verarbeitet, muss eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegen. Werden sensible Daten i. S. d. Art. 9 Abs. 1 DSGVO verarbeitet, ist die Verarbeitung grundsätzlich verboten, wenn nicht eine der in Art. 9 Abs. 2 DSGVO genannten Ausnahmen eingreift.

2. Der Anwendungsbereich der DSGVO ist indes nicht eröffnet, wenn Daten verarbeitet werden, die wirksam anonymisiert wurden, sodass der Personenbezug komplett aufgehoben und keine Re-Identifizierung mehr möglich ist.[1]

3. Der Vorgang des Anonymisierens ist dabei selbst eine Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO, sodass eine Rechtsgrundlage dafür vorliegen muss. Sensible Daten können nur unter den zusätzlichen Voraussetzungen des Art. 9 Abs. 2 DSGVO anonymisiert werden.

4. Soweit eine Anonymisierung technisch möglich ist, muss die Verantwortliche anonymisierte Daten verwenden, da sonst ein Verstoß gegen den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO vorliegt.[2]

5. Art. 6 Abs. 4 DSGVO regelt die Weiterverarbeitung von Daten, die zu einem anderen Zweck als demjenigen erfolgt, der ursprünglich für die Verarbeitung vorgesehen war. Voraussetzung für die Weiterverarbeitung ist, dass ursprünglicher und neuer Zweck

---

[1] Kapitel 6 B. (S. 117).
[2] Kapitel 6 B.II. (S. 121).

miteinander vereinbar sind. Die Vereinbarkeit wird anhand einer umfassenden Einzelfallabwägung unter Berücksichtigung der in Art. 6 Abs. 4 lit. a-f DSGVO aufgeführten Kriterien beurteilt. Die hohen Anforderungen werden beim Training algorithmischer Systeme regelmäßig nicht erfüllt sein, sodass die Verarbeitung personenbezogener Daten auf Grundlage des Art. 6 Abs. 4 DSGVO für Trainingszwecke ausscheidet.[3]

6. Sensible Daten i. S. d. Art. 9 Abs. 1 DSGVO dürfen grundsätzlich nur nach den Ausnahmetatbeständen des Art. 9 Abs. 2 DSGVO verarbeitet werden. In Art. 6 Abs. 4 lit. c DSGVO werden sensiblen Daten gem. Art. 9 Abs. 1 DSGVO indes ausdrücklich genannt. Somit sind sensible Daten im Rahmen von Art. 6 Abs. 4 lit. c DSGVO ein Abwägungs- und kein sofortiges Ausschlusskriterium. Je sensibler allerdings die personenbezogenen Daten sind, desto eher ist eine Weiterverarbeitung unzulässig.

7. Für Trainingszwecke ist die Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO keine rechtssichere Verarbeitungsgrundlage, da sie jederzeit frei widerruflich ist.[4] Der Widerruf kann im Extremfall dazu führen, dass die weitere Verwendung des maschinell lernenden Systems unzulässig wird, das mithilfe der Daten der widerrufenden Person trainiert wurde.

8. Verarbeitet man die personenbezogenen Daten zu Trainingszwecken auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f DSGVO, ist es ein milderes Mittel gegenüber der Verarbeitung personenbezogener Daten, wenn die Daten pseudonymisiert verarbeitet werden. Im Übrigen dürfen im Rahmen des Art. 6 Abs. 1 S. 1 lit. f DSGVO die Interessen der betroffenen Personen nicht überwiegen.

---

[3] Kapitel 6 B.IV.4. (S. 137).

[4] Kapitel 6 B.V. (S. 145).

9. Seit dem Urteil des EuGH vom 30. März 2023[5] ist § 26 Abs. 1 S. 1 BDSG nicht mehr anwendbar.[6] Werden personenbezogene Daten für ein konkretes Beschäftigungsverhältnis verarbeitet, ist nunmehr Art. 6 Abs 1 S. 1 lit. b DSGVO als Rechtsgrundlage heranzuziehen. Zentrales Merkmal des Art. 6 Abs. 1 S. 1 lit. b DSGVO ist die „Erforderlichkeit"[7]. Der Einsatz des maschinell lernenden Systems muss insoweit für den Verarbeitungszweck geeignet, erforderlich und angemessen sein.[8] Auf der Ebene der Angemessenheit sind das Interesse der Arbeitgeberin an der Datenverarbeitung und das Persönlichkeitsrecht der betroffenen Person gegeneinander abzuwägen. Dabei ist insbesondere zu berücksichtigen, dass Arbeitnehmerinnen nicht permanent überwacht werden dürfen, eine umfassende Persönlichkeitsprofilerstellung unzulässig ist und der betroffenen Person nicht ihre Individualität abgesprochen werden darf.[9]

10. Die Voraussetzungen einer Einwilligung der betroffenen Person werden für die Zwecke der Datenverarbeitung im konkreten Beschäftigungsverhältnis regelmäßig nicht erfüllt sein, da es an der Freiwilligkeit i. S. d. § 26 Abs. 2 BDSG fehlen wird.[10] Die Einwilligung kann außerdem jederzeit widerrufen werden. Deshalb ist die Einwilligung keine rechtssichere Rechtsgrundlage für die Datenverarbeitung im laufenden Beschäftigungsverhältnis.

11. Art. 88 Abs. 1 DSGVO räumt den Mitgliedstaaten im Beschäftigtendatenschutz eine autonome Regelungsbefugnis ein. Betriebsvereinbarungen können als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen.[11] Die Parteien einer Kollektivvereinbarung können richtigerweise vom prinzipiellen

---

[5] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659.

[6] Kapitel 5 B.II.1.c) (S. 87).

[7] Kapitel 6 C.IV. (S. 171).

[8] Kapitel 6 C.IV.2. (S. 172).

[9] Kapitel 6 C.IV.2.d)aa)(6) (S. 188).

[10] Kapitel 6 C.III.1. (S. 163).

[11] *Holthausen*, RdA 2021, 19, 32.

Schutzstandard des Art. 88 Abs. 2 DSGVO sowohl „nach unten“ als auch „nach oben“ abweichen.[12] Sie müssen allerdings die in Art. 5, 6, 9 DSGVO verankerten Prinzipien wahren und Art. 12 ff. DSVO berücksichtigen.

12. Wenn algorithmische Systeme unterstützend bei der Entscheidungsfindung eingesetzt werden, sind sie nicht nach Art. 22 Abs. 1 DSGVO unzulässig.[13] Art. 22 Abs. 1 DSGVO verbietet nur ausschließlich auf einer automatisierten Datenverarbeitung beruhende Entscheidungen.

13. Trotzdem sind automatisiert generierte Vorschläge, die zur Unterstützung der Entscheidung herangezogen werden, wegen ihres Einflusses auf die Entscheidungsträgerinnen gefährlich.[14] Sichergestellt werden muss daher, dass die Entscheidungsträgerinnen noch tatsächlich eine eigene Entscheidung vornehmen. Diese Eigenentscheidung muss zudem nachweisbar sein, z. B. durch ein Entscheidungsprotokoll, aus dem die berücksichtigten Kriterien hervorgehen.

14. Die Ausnahmen nach Art. 22 Abs. 2 DSGVO sind mit Blick auf Art. 22 Abs. 1 DSGVO eng auszulegen. Im Beschäftigungskontext wird eine Ausnahme nach Art. 22 Abs. 2 DSGVO fast nie einschlägig sein, da die einzelnen Voraussetzungen nur in Ausnahmefällen vorliegen werden.[15]

15. Nach Art. 13 Abs. 2 lit. f DSGVO, 14 Abs. 2 lit. g DSGVO sowie 15 Abs. 1 lit. h DSGVO hat die betroffene Person das Recht, aussagekräftige Informationen über die involvierte Logik sowie über die Auswirkungen der Datenverarbeitung zu erhalten.

---

[12] EuGH, 30.3.2023 – C-34/21, *Hauptpersonalrat./.Minister des Hessischen Kultusministeriums*, NVwZ 2023, 659, 661 Rn. 51; Kapitel 6 C.V.2. (S. 195).

[13] *Hoffmann-Riem* bezeichnet Art. 22 DSGVO daher als „stumpfes Schwert“, s. *Hoffmann-Riem*, in: Unger/Ungern-Sternberg (Hrsg.), Demokratie und künstliche Intelligenz, 2019, 148.

[14] Kapitel 6 D.IV.3.b) (S. 216).

[15] Kapitel 6 D.IV.5. (S. 224).

16. *De lege lata* gelten diese Informationspflichten nur für ausschließlich automatisierte Entscheidungen, die gem. Art. 22 Abs. 2 DSGVO unter bestimmten Voraussetzungen ausnahmsweise zulässig sind. [16] Bei arbeitsrechtlichen Auswahlentscheidungen sollten die Informationspflichten *de lege ferenda* nicht nur auf ausschließlich automatisierte Entscheidungen begrenzt sein. Denn auch ein entscheidungsunterstützend eingesetztes System kann sich wesentlich auf die menschliche Letztentscheidung auswirken.[17]

17. Die Informationen müssen gem. Art. 12 Abs. 1 S. 1 DSGVO in präziser und transparenter Form dargestellt sowie verständlich und leicht zugänglich präsentiert werden. Sie müssen daher auf den Empfängerhorizont der betroffenen Person zugeschnitten sein und dürfen keine irrelevanten Informationen enthalten. [18] Es ist nicht verpflichtend, Bildsymbole zu verwenden. *De lege ferenda* sollte es indes eine Pflicht zur Verwendung standardisierter Bildsymbole oder gar auch von Darstellungen per Video geben, damit die betroffene Person die wesentlichen Informationen tatsächlich zur Kenntnis nimmt.[19]

18. Ein Recht auf Begründung der Entscheidung ist nach der DSGVO nicht vorgesehen. Es ist aber sinnvoll, ein Recht auf Begründung in grundrechtssensiblen Bereichen einzuführen, um mehr Transparenz für die betroffene Person herzustellen.[20] Mithilfe von XAI ist es – jedenfalls in Teilen – bereits heutzutage möglich, bestimmte Entscheidungsprozesse maschinell lernender Systeme offenzulegen.[21]

---

[16] Kapitel 7 B.I. (S. 248).

[17] Kapitel 6 D.IV.3.b) (S. 216).

[18] Kapitel 7 B.IV.2. (S. 254).

[19] Kapitel 7 B.V.2. (S. 258).

[20] Kapitel 7 B.V.3. (S. 259); s. zum Recht auf Begründung nach Art. 68c KI-VO-PARL: Kapitel 11 F (S. 386).

[21] Kapitel 4 A.II. (S. 42).

Teil 3

Anforderungen nach dem AGG

Der nächste Teil widmet sich dem AGG. Ziel des AGG ist es, Benachteiligungen wegen bestimmter Gründe zu verhindern oder zu beseitigen, s. § 1 AGG. Die Existenz des AGG, insbesondere die Entschädigungs- und Schadensersatzregelung gem. § 15 AGG sorgt dafür, dass man Benachteiligungen nicht schutzlos ausgeliefert ist.[1]

Auch algorithmische Systeme können benachteiligen.[2] Daher soll im folgenden Abschnitt erörtert werden, welche Gründe es für Benachteiligungen gibt[3] und inwiefern gegen das Benachteiligungsverbot nach § 7 AGG verstoßen werden kann, wenn algorithmische Systeme eingesetzt werden[4]. Besondere Herausforderungen stellen sich im Rahmen von § 15 AGG: Hat eine Arbeitgeberin den Verstoß gegen ein Benachteiligungsverbot gem. § 15 Abs. 1 S. 1 AGG zu vertreten, wenn ein algorithmisches System eingesetzt wurde?[5] Für die Arbeitnehmerin hingegen ist es schwierig, Indizien gem. § 22 AGG vorzubringen, wenn ein maschinell lernendes System eingesetzt wurde: Häufig sind solche Systeme nicht ohne Weiteres transparent.[6] An dieser Stelle zeigt die Arbeit einen Lösungsvorschlag auf.

---

[1] *Benecke*, in: Brose/Greiner/Rolfs u.a. (Hrsg.), Grundlagen des Arbeits- und Sozialrechts, 2021, 73.

[2] Kapitel 8 A. (S. 281).

[3] Kapitel 8 B. (S. 288).

[4] Kapitel 9 A. (S. 293).

[5] Kapitel 9 B. (S. 310).

[6] S. dazu bereits unter: Kapitel 4 A. (S. 40).

Kapitel 8

Benachteiligung durch algorithmische Systeme

A. Mögliche Benachteiligungen

Laut einer Befragung aus dem Jahr 2018 sind zwei Drittel von knapp 200 Unternehmen der Top 1000 und Top 300 IT-Unternehmen der Meinung, dass durch eine automatisierte Vorauswahl von Bewerbungen dieser Vorgang diskriminierungsfreier wird, es nutzen aber nur 6 % der IT-Unternehmen die Möglichkeit einer automatisierten Bewerberinnenvorauswahl.[1]

Werden algorithmische Systeme eingesetzt, können sich Benachteiligungen für bestimmte Gruppen ergeben.[2] Um zu zeigen, welche Folgen diskriminierende Systeme nach sich ziehen, werden zunächst drei Negativbeispiele erläutert.

I. Bewerbungssystem filtert bestimmte Gruppen heraus

Ein Negativbeispiel ist das algorithmische System vom US-Konzern *Amazon*, welches aus vielen Lebensläufen geeignete Kandidatinnen herausfiltern sollte.[3] Das System gab den Lebensläufen eine Bewertung von null bis fünf Sternen, auf dessen Basis die Personen eingestellt wurden. Trainiert wurde das System mit Lebensläufen, die in den letzten zehn Jahren

---

[1] *Gärtner*, Smart HRM, 2020, S. 8; *Laumer/Weitzel/Luzar*, PERSONALquaterly 2019, 10.

[2] Zur Diskriminierung in der Medizin s. *Baumgartner*, in: Bauer/Kechaja/Engelmann u.a. (Hrsg.), Diskriminierung und Antidiskriminierung, 2021, S. 160; *Beck*, Künstliche Intelligenz und Diskriminierung: Herausforderungen und Lösungsansätze, 2019, S. 5 f.; *European Union Agency for Fundamental Rights*, Bias in algorithms – Artificial intelligence and discrimination, 08.12.2022.

[3] The Guardian, Amazon ditched AI recruiting tool that favored men for technical jobs, https://perma.cc/AGN3-S6DJ (archiviert am 18.01.2023).

eingereicht worden waren. Die meisten der Lebensläufe kamen von Männern. Das System schloss aus den Daten, dass männliche Kandidaten wünschenswerter sind. Heruntergestuft wurden daher Lebensläufe, die z. B. das Wort „Frau" enthielten. Frauen wurden schlechter bewertet, weil das Geschlecht als Kriterium dem System unbekannt war.[4]

In einem anderen Fall sortierte ein maschinell lernendes System Bewerberinnen aus, die weiter von der Arbeitsstätte entfernt wohnten.[5] Es hatte festgestellt, dass diese Menschen häufiger kündigten. Da außerhalb vom Stadtzentrum häufig Menschen wohnen, die einer ethnischen Minderheit angehören, wurde auch bei diesem Beispiel eine bestimmte Gruppe von Bewerberinnen diskriminiert.[6]

II. Negativbeispiel *COMPAS*

Das US-amerikanische Justizsystem setzt in einigen Bundesstaaten die Software *COMPAS („Correctional Offender Management Profile for Alternative Sanctions")* ein, das bereits verurteilte Straftäterinnen nach ihrem prognostizierten Rückfallrisiko einordnet.[7] *COMPAS* wird momentan in fünf US-Bundesstaaten eingesetzt.[8]

Auf der Grundlage sämtlicher Informationen über die straffälligen Personen kann das algorithmische System herausfinden, welche Informationen mit der Rückfälligkeit einer Straftäterin korrelieren, etwa das Alter und das Geschlecht.[9] Dabei untersucht das System nicht nur einzelne Informationen auf ihren Einzeleffekt hin, sondern berücksichtigt auch größere Teilmengen von Informationen. Die Korrelationen werden entsprechend gewichtet und

---

[4] Spiecker gen. Döhmann/Bretthauer/*Spiecker gen. Döhmann/Bretthauer*, G 2.4.81 I.; *Höpfner/Daum*, ZfA 2021, 467, 491.

[5] S. dazu auch: *Dzida/Groh*, NJW 2018, 1917, 1919.

[6] *Wilke*, Künstliche Intelligenz diskriminiert (noch), Zeit Online, 18.10.2018, https://perma.cc/T8AM-KFX9 (archiviert am 05.12.2022).

[7] *Northpointe Inc.*, Practitioner's Guide to COMPAS Score, 2019, S. 1.

[8] *Räz*, Forens Psychiatr Psychol Kriminol 16 (2022), 300, 301; *Electronic Privacy Information Center*, Liberty at Risk: Pre-trial Risk Assessment Tools in the U.S., 2020, https://perma.cc/4TEE-BJST (archiviert am 05.12.2022).

[9] *Krafft/Zweig*, in: Kar/Thapa/Parycek (Hrsg.), (Un)berechenbar?, 2018, 476.

durch den Algorithmus abgebildet.[10] Die Einordnung der Straftäterinnen erfolgt anhand eines *Scoring*-Werts in drei Risikogruppen: Je nach *Score* wird den Personen ein niedriges, mittleres oder hohes Risiko zugeschrieben.[11]

Warum ist die Software kritisch zu betrachten? Die Qualität der Software gibt das Unternehmen mit 70 % an.[12] Um diese zu messen, verwendet das Unternehmen die sogenannte *Receiver-Operator Characteristic Area under the curve (ROC AUC)*. Die ROC AUC ist eines der bekanntesten Qualitätsmaße im Bereich des maschinellen Lernens und gibt in dem Fall von *COMPAS* an, wie viele Paare von „rückfälligen" und „nicht-rückfälligen" Personen korrekt sortiert worden sind.[13] Ein Paar ist immer dann korrekt sortiert worden, wenn derjenigen Person ein höheres Rückfallrisiko zugesprochen wird, die auch tatsächlich rückfällig geworden ist.[14] Im Fall von *COMPAS* kam man zu dem Ergebnis, dass 70% der Paare richtig einsortiert wurden.

Katharina Zweig und *Tobias Krafft* verwenden in ihrer Forschung hingegen ein anderes Qualitätsmaß, nämlich den *Positive Predictive Value (PPVk).*[15] Der PPVk gibt an, wie viele Personen, die die höchsten *Scoring*-Werte erhalten haben und somit in der Kategorie „hohes Risiko" eingeordnet wurden, tatsächlich rückfällig geworden sind.[16] Das „k" des PPVk entspricht der bekannten Anzahl von rückfälligen Personen im Datenset. In dem von *Zweig* und *Krafft* verwendeten Datensatz befanden sich zehn rückfällige Personen. Unter den Personen mit den höchsten *Scoring*-Werten waren aber nur fünf rückfällige Personen: Der PPVk-Wert lag somit nur bei 50 %. Mithin lag die Qualität nach diesem Qualitätsmaß nicht bei den erwähnten 70 % des Unternehmens.

Die beiden Qualitätsmaße treffen unterschiedliche Aussagen über einen Datensatz. Der ROC AUC zeigt, wie gut ein Algorithmus in der Lage ist, aus

---

[10] *Ebd.*, 477.
[11] *Ebd.*, 477.
[12] *Ebd.*, 479.
[13] *Ebd.*, 480.
[14] *Ebd.*,, 480.
[15] *Ebd.*, 480.
[16] *Ebd.*, 480.

Paaren von Kandidatinnen die vermeintlich rückfällig gewordene Kandidatin zu bewerten; der PPVk misst hingegen, ob der Algorithmus derjenigen einen hohen Wert zumisst, die auch tatsächlich rückfällig werden.[17]

Es macht somit einen erheblichen Unterschied, welches Qualitätsmaß man zugrunde legt, um die Aussagekraft eines Systems zu messen.

III. Arbeitsmarkt-Chancen-Modell aus Österreich

Ein weiteres, als kritisch einzustufendes Beispiel für den Einsatz von KI stammt aus Österreich. Dort beschlossen Verwaltungsrat und Vorstand des *Arbeitsmarktservice* (AMS) im Frühjahr 2018 ein System zu entwickeln, das die Integrationschancen arbeitssuchender Personen bewerten kann.[18] Die erste Version im Oktober 2018 war der *AMS*-Algorithmus, auch Arbeitsmarkt-Chancen-Modell genannt. Die aktualisierte Version wurde Anfang des Jahres 2020 unter der Bezeichnung „Assistenzsystem AMAS" veröffentlicht.[19] Momentan wird *AMAS* nicht eingesetzt.[20]

1. Funktionsweise des AMAS

Zur Berechnung der Chancen der betroffenen Personen auf dem Arbeitsmarkt werden verschiedene Datenkategorien der Arbeitssuchenden verarbeitet: persönliche Merkmale wie Alter, Geschlecht, Staatsbürgerschaft, Ausbildung, gesundheitliche Einschränkungen, Betreuungspflichten, Berufsgruppe; zudem der bisherige Erwerbsverlauf und der aktuelle Geschäftsfall.[21] Der Begriff des Geschäftsfalls wird nicht näher definiert. Es liegt aber nahe, dass ein Geschäftsfall jeden Vorgang meint, in dem die

---

[17] *Ebd.*, 481.

[18] *Büchner/Dosdall*, KZfSS 2021, 333, 337; umfassend zum *AMAS* s. *Allhutter/Cech/Fischer u.a.*, Frontiers in big data 2020; *Krause*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 143.

[19] *Büchner/Dosdall*, KZfSS 2021, 333, 337.

[20] *Krause*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 143, 146.

[21] *Holl/Kernbeiß/Wagner-Pinter*, Das AMS-Arbeitsmarktchancen-Modell, 2018, S. 3; *Karaarduc*, EALR 2021, 35, 37.

Arbeitsagentur in Bezug auf eine bestimmte Beschäftigte oder arbeitssuchende Person tätig wird.

Der Algorithmus wurde mithilfe bereits vorhandener Daten trainiert. Diese Daten wurden aber nicht deshalb ausgewählt, weil sie qualitativ besonders hochwertig waren, sondern weil sie verfügbar waren.[22]

Die Arbeitslosen werden in Gruppen sortiert. Insgesamt gibt es drei Gruppen, in die die Arbeitssuchenden eingeteilt werden: gute Chancen (A), mittlere Chancen (B) und schlechte Chancen (C).[23] Das Ergebnis des Algorithmus unterstützt die Beraterinnen des *AMS* bei der Entscheidung, wie weiter mit den Arbeitslosen zu verfahren ist.[24]

Das System wurde von Forscherinnen bereits in der Testphase erheblich kritisiert: Bestimmte Personengruppen (z. B. Frauen) würden benachteiligt werden.[25] Zudem werde nicht hinreichend offengelegt, wie groß die Fehlerquote bei einzelnen Testabläufen ausfalle. Hinzu komme, dass auch nicht klar sei, wie groß der Entscheidungsspielraum einzelner Arbeitnehmerinnen des *AMS* sei, die die Entscheidung auf Grundlage des Ergebnisses des Systems träfen.[26]

2. Untersagung von der Datenschutzbehörde

Anfang 2021 sollte das Modell landesweit eingeführt werden; die Datenschutzbehörde in Österreich verhinderte jedoch mit Bescheid vom 16. August 2020[27] den landesweiten Einsatz. Durch das Modell werde

---

[22] *Büchner/Dosdall*, KZfSS 2021, 333, 338.

[23] *Wimmer*, Was der neue AMS-Algorithmus für Frauen wirklich bedeutet, future zone, 28.09.2019, https://perma.cc/X6GC-X2T7 (archiviert am 02.08.2022).

[24] *Köver*, Wenn Maschinen über Menschen entscheiden, Netzpolitik.org, 10.05.2022, https://perma.cc/FV57-KQAR (archiviert am 02.08.2022).

[25] *Allhutter/Cech/Fischer u.a.*, Frontiers in big data 2020, 3.1.2. Bias and Discrimination; *Arbeit plus*, Algorithmen und das AMS Arbeitsmarkt-Chancen-Modell, 2019, S. 6; *Karaarduc*, EALR 2021, 35, 39.

[26] *Cech/Fischer/Human/Lopez/Wagner*, Dem AMS-Algorithmus fehlt der Beipackzettel, future zone, 03.10.2019, https://perma.cc/9264-HTRC (archiviert am 02.08.2022).

[27] *Datenschutzbehörde Österreich*, ZIIR 2020, 410-416.

„eingriffsrelevantes Profiling betrieben", für das erst eine Rechtsgrundlage geschaffen werden müsse.[28] Zwar dürfe man gem. § 25 Abs. 1 AMSG bestimmte Datenarten verarbeiten. Für den Rechtsunterworfenen sei aber nicht nachvollziehbar, dass auf Grundlage des § 25 Abs.1 AMSG die Datenarten zum Zwecke der Bewertung von Arbeitsmarktchancen verarbeitet würden.[29] Je gravierender der Eingriff in das Grundrecht auf Datenschutz sei, desto eher müsse der Eingriff für die Betroffenen vorhersehbar sein und umso strenger werde der Maßstab, dass die Rechtsgrundlagen klar und präzise formuliert sein und für die Rechtsunterworfene in ihren Anwendungsfällen vorhersehbar sein müssten.[30] Das sei im Fall des *AMS*-Algorithmus nicht gewährleistet, sodass für die Datenverarbeitung durch den *AMS*-Algorithmus daher keine ausreichende Rechtsgrundlage bestehe.[31]

Hinzu komme, dass gegen Art. 22 Abs. 1 DSGVO verstoßen werde: Aufgrund der Ausnahmesituation wegen der Covid-19-Pandemie und – damit verbunden – nicht persönlich stattfindender Gespräch des *AMS*, sei davon auszugehen, dass die Ergebnisse des *AMS*-Algorithmus durch die Arbeitnehmerinnen uneingeschränkt übernommen würden.[32] Jedenfalls würden die Position der Arbeitnehmerinnen durch die Ergebnisse in einem derart hohen Grad beeinflusst werden, dass durch die Datenverarbeitung mithilfe des *AMS*-Algorithmus von einer „erheblichen Beeinträchtigung" i. S. d. Art. 22 Abs. 1 DSGVO auszugehen sei.[33]

---

[28] *Köver*, Wenn Maschinen über Menschen entscheiden, Netzpolitik.org, 10.05.2022, https://perma.cc/FV57-KQAR (archiviert am 02.08.2022).

[29] *Datenschutzbehörde Österreich*, ZIIR 2020, 410-416, 414 ff.; *Zavadil*, Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen, 2020, S. 3.

[30] *Zavadil*, Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen, 2020, S. 3.

[31] *Ders.*, Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen, 2020, S. 4.

[32] *Ders.*, Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen, 2020, S. 4.

[33] *Datenschutzbehörde Österreich*, ZIIR 2020, 410-416, 415 ff.; *Zavadil*, Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen, 2020, S. 4.

3. Kassation des Verbots durch das BVwG Österreich

Mit Urteil vom 18.12.2020 wurde das Verbot des *AMS*-Modells mit Wirkung zum 1.1.2021 wieder aufgehoben.[34] Die Datenverarbeitung könne auf § 25 Abs. 1 AMSG gestützt werden. Es gebe keine Anhaltspunkte dafür, dass eine Verarbeitung bestimmter personenbezogener Daten nach § 25 AMSG nicht hinreichend ersichtlich sei und auch sonst nicht anhand angemessener und spezifischer Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen geregelt sei. Auch liege kein Verstoß gegen Art. 22 DSGVO vor.[35] Die finale Entscheidung träfen die Beraterinnen des *AMS*; die Entscheidung beruhe somit nicht ausschließlich auf einer automatisierten Verarbeitung. Selbst wenn Arbeitnehmerinnen das Ergebnis des *AMAS* übernehmen würden und damit gegen verbindliche Vorgaben des Arbeitsmarktservice verstoßen würden, sei das nicht relevant für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung. Dass spezifische geeignete Maßnahmen fehlten, um die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten, müsste gesondert gerügt und in einem neuen Verfahren überprüft werden.

Aus einer Parlamentskorrespondenz[36] vom 8.11.2022 geht hervor, dass das Tool unabhängig vom Ausgang der höchstrichterlichen Entscheidung neu analysiert werden soll.[37]

---

[34] BVwG Österreich, 18.12.2020, ECLI:AT:BVWG:2020:W256.2235360.1.00.

[35] BVwG Österreich, 18.12.2020, ECLI:AT:BVWG:2020:W256.2235360.1.00; kritisch dazu s. *Krause*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 143, 153; *Gerhartl*, ZIIR 2021, 24, 28 f.

[36] Die Parlamentskorrespondenz berichtet „objektiv, umfassend und parteiunabhängig" über das Geschehen im Hohen Haus (Parlament in Österreich), https://perma.cc/NB9X-MLWE (archiviert am 21.5.2023).

[37] Parlamentskorrespondenz Nr. 1249 vom 08.11.2022, https://perma.cc/7C4L-LK4M (archiviert am 05.12.2022).

B. Gründe für eine Benachteiligung durch Algorithmen

Die Beispiele zeigen: Algorithmische Entscheidungen können diskriminierend wirken. Die Gründe für die Benachteiligung sind vielfältig:[38]

I. Mangelnde Qualität der Trainingsdaten

Die Ungleichbehandlung zweier Gruppen kann bereits in den Trainingsdaten vorhanden sein und durch den Einsatz des maschinell lernenden Systems verstärkt werden.[39] Werden zu dem Verb „kochen" überwiegend Bilder mit Frauen gezeigt, wird das System das entsprechend abbilden und die Assoziation durch weitere Anwendung verstärken.[40] In dem oben genannten Beispiel des algorithmischen Systems von *Amazon* war die Gruppe weiblicher Bewerberinnen unterrepräsentiert, was in der Anwendung weibliche Bewerberinnen benachteiligt hat. Um das zu verhindern, kann der Trainingsdatensatz ausbalanciert werden, indem entweder Datenpunkte der Mehrheitsgruppe nicht berücksichtigt werden (*sog. undersampling*) oder künstliche Datenpunkte der unterrepräsentierten Gruppe verwendet werden

---

[38] *Bär*, Algorithmic Bias: Verzerrungen durch Algorithmen verstehen und verhindern, 2022, S. 57 ff.; *Beck*, Künstliche Intelligenz und Diskriminierung: Herausforderungen und Lösungsansätze, 2019, S. 8; *Berendt*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 31, 38 ff.; *Müller*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 205, 208; *Lang/Reinbach*, NZA 2023, 1273, 1274; *Lauscher/Legner*, ZfDR 2022, 367, 371 f.; *Veale/Binns*, Big Data & Society 4 (2017), 1-17, 2 f.

[39] *Berendt*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 31, 38; *Hacker*, Law, Innovation and Technology 13 (2021), 257, 261; *Heesen/Reinhardt/Schelenz*, in: Bauer/Kechaja/Engelmann u.a. (Hrsg.), Diskriminierung und Antidiskriminierung, 2021, 134 f.; *Lauscher/Legner*, ZfDR 2022, 367, 371; *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 25.

[40] *Gesellschaft für Informatik*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, 2018, S. 35.

(*sog. oversampling*).[41] Solche Korrekturen der Datensätze haben aber auch Nachteile: Die Vorhersagegenauigkeit des Systems nimmt ab.[42]

II. Berücksichtigung von *Proxy*-Variablen

Wie bereits dargelegt worden ist, ergeben sich Benachteiligungen häufig dadurch, dass eine Korrelation zwischen einem geschützten Merkmal und einem an sich neutralen Merkmal hergestellt wird.[43] Der ethnische Hintergrund korreliert z. B. häufig mit dem Wohnort.[44] Eine Benachteiligung ergibt sich häufig daraus, dass eine an sich harmlose Information (sog. *proxy*) mit einem verpönten Merkmal korreliert.[45] Das wird auch als statistische Diskriminierung verstanden, d. h. die „ungerechtfertigte Ungleichbehandlung von Personen mithilfe von Ersatzinformationen".[46] Beispielsweise besteht beim Merkmal „Teilzeitbeschäftigung" die Gefahr einer mittelbaren statistischen Diskriminierung: Teilzeit korreliert mit dem geschützten Merkmal „Geschlecht", da Frauen häufiger als Männer in Teilzeit arbeiten.[47] Ähnlich wie in dem oben genannten Beispiel nutzte der Dienstleister *Xerox Services* die Informationen zum Anfahrtsweg der Bewerberinnen zur automatischen Aussortierung von Kandidatinnen: Bei zu langen Anfahrtswegen wurden Kandidatinnen abgelehnt, weil Arbeitnehmerinnen mit längeren Anfahrtswegen statistisch gesehen schneller kündigten als Arbeitnehmerinnen mit kürzeren Anfahrtswegen. Dieses Kriterium

---

[41] *Dies.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, 2018, S. 35.

[42] *Dies.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, 2018, S. 35.

[43] Kapitel 3 C. (S. 36); *Gössl*, in: Diskriminierungsfreie KI, 2023, S. 3, 13.

[44] *Martini*, Blackbox Algorithmus, 2018, S. 73 Fn. 202.

[45] *Barocas/Selbst*, Cal. L. Rev. 2016, 671, 691; *Braun Binder/Spielkamp/Egli u.a.*, Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen, 2021, S. 41; *Müller*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 205, 216 f.; *Lauscher/Legner*, ZfDR 2022, 367, 372 f.

[46] *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen (2020), S. 27.

[47] *Ebd.*, S. 28.

diskriminierte Menschen aus ärmeren Vierteln mit vorrangig schwarzer Bevölkerung, weil sie sich zentrale Wohnungen nicht leisten können.[48]

Am einfachsten wäre es daher, derartige Merkmale nicht zu berücksichtigen. Problematisch ist allerdings, dass viele Merkmale für sich genommen vermeintlich „harmlos" sind und somit nicht alle potenziell zu Benachteiligungen führenden Merkmale erkannt werden. Außerdem führt die Nichtberücksichtigung derartiger Merkmale dazu, dass das System zu ungenauen Ergebnissen führt.[49]

III. Vorurteile der Entwicklerinnen und Wahl der Parameter

Die Entwicklerinnen algorithmischer Systeme sind auch nicht frei von Vorurteilen. Ihre Vorurteile, Wertvorstellungen und Ansichten schlagen sich auch im System nieder und können zu Benachteiligungen führen.[50] Wie Daten analysiert werden, wird schließlich auch durch Entwicklerinnen vorgegeben.[51] Man sollte also versuchen, möglichst divers besetze Entwicklungsabteilungen zu haben, damit verschiedene Auffassungen und Ansichten mit in die Entwicklung algorithmischer Systeme einfließen.[52] Zwar garantiert ein divers besetztes Entwicklungsteam nicht, dass alle Bedürfnisse und Anforderungen unterschiedlicher gesellschaftlicher Gruppen berücksichtigt werden.[53] Allerdings werden jedenfalls mehr Anforderungen berücksichtigt, je diverser das Entwicklungsteam ist. Für ein rein männlich besetztes Entwicklungsteam

---

[48] *Lischka/Klingel*, Wenn Maschinen Menschen bewerten, 2017, S. 22.

[49] *Gesellschaft für Informatik*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, 2018, S. 36.

[50] Umfassend dazu s. *Bär*, Algorithmic Bias: Verzerrungen durch Algorithmen verstehen und verhindern, 2022, S. 65 ff.; *Beck*, Künstliche Intelligenz und Diskriminierung: Herausforderungen und Lösungsansätze, 2019, S. 8; *Wischmeyer*, AöR 143 (2018), 1, 27.

[51] *Martini*, Blackbox Algorithmus, 2018, S. 46.

[52] *Heesen/Reinhardt/Schelenz*, in: Bauer/Kechaja/Engelmann u.a. (Hrsg.), Diskriminierung und Antidiskriminierung, 2021, 138; vgl. *Martini*, Blackbox Algorithmus, 2018, S. 49.

[53] *Heesen/Reinhardt/Schelenz*, in: Bauer/Kechaja/Engelmann u.a. (Hrsg.), Diskriminierung und Antidiskriminierung, 2021, S. 139.

kann es z. B. schwierig sein, die Anforderungen von Frauen in einem bestimmten Anwendungsfall zu antizipieren.[54]

Außerdem kann die Wahl der Parameter ausschlaggebend dafür sein, ob das algorithmische System Benachteiligungen hervorruft. Muss man definieren, was eine „gute Arbeitnehmerin" ausmacht, gibt es dafür verschiedene Ansätze, aber es existiert nicht der eine richtige Ansatz.[55] Soll etwa die mögliche Dauer der Betriebszugehörigkeit ein Grund für die Auswahl von geeigneten Bewerberinnen sein, kann es sein, dass Bewerberinnen einer bestimmten Gruppe benachteiligt werden, weil die Abbruchquote grundsätzlich eher höher ausfällt. Man kommt zu anderen Ergebnissen, wenn man etwa die Produktivität der Bewerberinnen als Auswahlkriterium nimmt.[56]

C. Zwischenergebnis: Benachteiligungen als Alltagsphänomen

1. Die Untersuchung zeigt, dass Benachteiligungen durch algorithmische Systeme bereits ein alltägliches Phänomen sind und erhebliche Auswirkungen auf einzelne Individuen haben können. Während einer Person mithilfe von *COMPAS*[57] womöglich ein falsches Rückfallrisiko zugeschrieben wird, kann die Beurteilung mithilfe des *AMAS*[58] dazu führen, dass die betroffene Person schlechtere Chancen auf dem Arbeitsmarkt hat.

2. Die Gründe für die Benachteiligung mittels algorithmischer Systeme sind vielfältig.[59] Insbesondere kann die Benachteiligung auf mangelnde Trainingsdatenqualität zurückzuführen sein. Weiter kann die Berücksichtigung von *Proxy*-Variablen zu einer Benachteiligung führen.

---

[54] *Ebd.,* S. 138.

[55] *Barocas/Selbst*, Cal. L. Rev. 2016, 671, 679 f.

[56] *Dies.*, Cal. L. Rev. 2016, 671, 680; S. dazu auch: *Müller*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 205, 210.

[57] Kapitel 8 A.II. (S. 282).

[58] Kapitel 8 A.III. (S. 284).

[59] Kapitel 8 B. (S. 288).

Schließlich können auch Vorurteile der Entwicklerinnen und die Wahl der Parameter dazu führen, dass ein benachteiligendes Ergebnis mithilfe des algorithmischen Systems hervorgerufen wird.

Kapitel 9

Schutzrahmen des AGG

A. Verstoß gegen das Benachteiligungsverbot

Vom Schutzbereich des AGG sind Ungleichbehandlungen aufgrund folgender Merkmale erfasst: ethnische Herkunft, Geschlecht, Religion, Weltanschauung, Behinderung, Alter oder sexuelle Identität. Wegen dieser in § 1 AGG genannten Gründe dürfen Beschäftigte gem. § 7 AGG nicht benachteiligt werden. Voraussetzung ist, dass der Anwendungsbereich des AGG eröffnet ist, eine Benachteiligung wegen eines in § 1 AGG genannten Grundes vorliegt und die Benachteiligung nicht gerechtfertigt ist.

I. Anwendungsbereich des AGG

1. Anwendungsbereich eröffnet beim Bezug zum Arbeitsverhältnis

In sachlicher Hinsicht ist der Anwendungsbereich des AGG unter anderem bei Benachteiligungen wegen eines in § 1 AGG genannten Grundes im Hinblick auf Auswahlkriterien und Einstellungsbedingungen sowie für den beruflichen Aufstieg (§ 2 Abs. 1 Nr. 1 AGG) eröffnet.[1] Algorithmische Systeme, die im Bewerbungsverfahren oder bestehenden Arbeitsverhältnis eingesetzt werden, enthalten Auswahlkriterien und Einstellungsbedingungen für das Arbeitsverhältnis oder den beruflichen Aufstieg, indem sie Persönlichkeitsanalysen oder Auswertungen von Lebensläufen oder sonstigen Dokumenten vornehmen.[2] Auch Entlassungsbedingungen werden nach § 2 Abs. 1 Nr. 2 AGG vom Anwendungsbereich erfasst. Derartige Bedingungen

---

[1] S. zur Erweiterung des Anwendungsbereichs des § 2 AGG auf Verbraucherverträge, bei denen die Vertragsbedingungen gegenüber einem Verbraucher auf *Scoring* oder *Profiling* zurückgehen, *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 75.

[2] *Dzida/Groh*, NJW 2018, 1917, 1918; *Sesing/Tschech*, MMR 2022, 24, 25.

erfassen alle Umstände, die eine Beendigung des Arbeitsverhältnisses beeinflussen.[3] Soll ein algorithmisches System mithin aufgrund von Kriterien eine Kündigungsmöglichkeit einer Bewerberin vorhersagen, wird das auch vom Anwendungsbereich des AGG erfasst.

Für Bewerberinnen ist das AGG nach § 6 Abs. 1 S. 2 AGG persönlich anwendbar. Die Eigenschaft als „Bewerberin" wird formal danach bestimmt, ob eine Bewerbung eingereicht wurde oder nicht.[4] Reichen Bewerberinnen somit eine Bewerbung ein – auch mittels eines algorithmischen Systems –, ist der Anwendungsbereich in persönlicher Hinsicht eröffnet. Für Arbeitnehmerinnen ist der Anwendungsbereich in persönlicher Hinsicht nach § 6 Abs. 1 Nr. 1 AGG eröffnet.

2. Anwendungsbereich eröffnet bei der Sammlung von Trainingsdaten

Eine Frage ist, wie mit Trainingsdaten im Antidiskriminierungsrecht umgegangen wird. Wie bereits an einigen Stellen der Arbeit deutlich geworden ist[5], hängt die Qualität der Ergebnisse mit der Qualität der Trainingsdaten zusammen. Grundsätzlich ist der Anwendungsbereich nach § 2 Abs. 1 AGG nicht bereits eröffnet, wenn man Trainingsdaten für maschinell lernende Systeme sammelt: [6] Für sich genommen sind Trainingsdaten keine Bedingungen nach § 2 Abs. 1 Nr. 1 AGG, die für den Zugang zu unselbstständiger und selbstständiger Erwerbstätigkeit relevant sind. Auch andere in § 2 Abs. 1 AGG genannte Fälle sind nicht einschlägig. Verzerrungen in den Trainingsdaten sind noch keine rechtlich relevante Benachteiligung.

Dennoch kann – wie bereits ausgeführt – durch mangelnde Qualität der Trainingsdaten beim späteren Einsatz eines maschinell lernenden Systems eine (mittelbare) Benachteiligung hervorgerufen werden.[7]

---

[3] ErfK/*Schlachter*, § 2 AGG Rn. 9.
[4] ErfK/*dies.*, § 6 AGG Rn. 3.
[5] S. etwa: Kapitel 6 C.IV.2.b)aa) (S. 176); Kapitel 8 B.I. (S. 288); Kapitel 10 B.I. (S. 345).
[6] *Hacker*, ZGE 2020, 240, 251.
[7] Kapitel 8 B.I. (S. 288).

Deshalb stellt sich die Frage, ob sich der Schutzbereich des AGG bereits auf die Zusammenstellung der Trainingsdaten erstreckt. Anhaltspunkte dafür bietet ein Urteil des EuGH.[8] In dem konkreten Fall tätigte ein Rechtsanwalt in einem Interview die Aussage, dass er homosexuelle Personen in seiner Anwaltskanzlei weder einstellen noch beschäftigen wolle.[9] Das Landgericht Bergamo verurteilte den Kläger zu Schadensersatz in Höhe von 10.000 € an die *associazione Avvocatura per i diritti LGBTI – Rete Lenford*. Diese ist eine Vereinigung von Rechtsanwälten, die Lesben, Schwulen, Bisexuellen, Transgendern und Intersexuellen vor Gericht Beistand leistet. Der Anwalt legte dagegen Kassationsbeschwerde ein und machte eine unzutreffende Anwendung des einschlägigen italienischen Rechts geltend. Er habe die Äußerung nicht als Arbeitgeber, sondern als Bürger getätigt. Die streitigen Äußerungen stünden daher außerhalb jedes tatsächlichen beruflichen Kontexts. Der EuGH entschied, dass der Begriff „Bedingungen für den Zugang zu [einer] Erwerbstätigkeit" i. S. v. Art. 3 Abs. 1 lit. a. der Richtlinie 2000/78 weit auszulegen sei: Auch bestimmte Äußerungen der Arbeitgeberin können bereits eine Bedingung für den Zugang zu einer Erwerbstätigkeit darstellen, wenn sie mit der Einstellungspolitik tatsächlich in Zusammenhang gebracht werden können. [10] Es komme nicht darauf an, ob ein Einstellungsverfahren tatsächlich geplant war oder bereits angelaufen ist; es komme lediglich darauf an, dass die Verbindung der Äußerungen zu den Bedingungen für den Zugang zu einer Erwerbstätigkeit in dem jeweiligen Unternehmen nicht hypothetisch sei. [11] Das müsse anhand einer Gesamtwürdigung geprüft werden.[12]

Die aufgestellten Maßstäbe lassen sich auf die Sammlung von Trainingsdaten übertragen: Werden Trainingsdaten ohne einen konkreten Bezug zum Anwendungsbereich des AGG gesammelt, wird der Anwendungsbereich noch nicht eröffnet sein. Es fehlt an einer entsprechenden Verbindung

---

[8] EuGH, 23.4.2020 – C-507/18, *Associazione Avvocatura per i diritti LGBTI ./. Rete Lenford.*

[9] EuGH, 23.4.2020 – C-507/18, *Associazione Avvocatura per i diritti LGBTI ./. Rete Lenford,* juris, Rn. 18.

[10] *Ebd*., Rn. 43.

[11] *Ebd*., Rn. 58.

[12] *Ebd*., Rn. 43.

zwischen den Daten und dem Anwendungsbereich des AGG. Werden aber Daten gesammelt, um ein maschinell lernendes System zu trainieren, welches im nächsten Bewerbungsprozess eingesetzt werden soll, geht es gerade um Szenarien, die in den Anwendungsbereich des AGG fallen werden.[13] Das maschinell lernende System legt in dem Fall Bedingungen fest, die für den Zugang zu unselbständiger und selbständiger Erwerbstätigkeit relevant sind (§ 2 Abs. 1 Nr. 1 AGG). In solchen Fällen überzeugt es daher, den Anwendungsbereich des AGG bereits auf die Sammlung von Trainingsdaten zu erstrecken.[14] Allerdings ist ein solches Verbandsklagerecht in Deutschland (noch) nicht vorgesehen, sodass es bislang keine Möglichkeit gibt, gegen potentielle Benachteiligungen vorzugehen.[15]

II. Verstoß gegen das Benachteiligungsverbot

1. Unmittelbare Benachteiligung

Das AGG differenziert zwischen zwei Arten der Benachteiligung: unmittelbarer und mittelbarer Benachteiligung. Nach § 3 Abs. 1 AGG liegt eine unmittelbare Benachteiligung vor, wenn eine Person wegen eines in § 1 AGG genannten Grundes eine weniger günstige Behandlung erfährt, als eine andere Person in einer vergleichbaren Situation erfährt, erfahren hat oder erfahren würde.

a) Behandlung durch ein algorithmisches System

Fraglich ist zunächst, ob das benachteiligende Ergebnis eines algorithmischen Systems überhaupt eine Behandlung i. S. d. § 3 Abs. 1 AGG sein kann.[16] Grundsätzlich wird unter Behandlung ein menschliches Tun oder Unterlassen verstanden.[17] Das relevante Tun oder Unterlassen ist bei der Bewerberinnenauswahl etwa die Einstellung, die Einladung zu einem Bewerbungsgespräch oder die Nichteinladung zu einem

---

[13] *Hacker*, ZGE 2020, 240, 252.
[14] I. E. auch: *ders.*, Law, Innovation and Technology 13 (2021), 257, 274.
[15] *Herberger*, RdA 2022, 220.
[16] *Lewinski/Barros Fritz*, NZA 2018, 620, 621.
[17] BeckOK Arbeitsrecht/*Roloff*, § 3 AGG Rn. 2.

Bewerbungsgespräch.[18] Final nimmt diese Handlungen ein Mensch vor. Eine vollständig automatisierte Entscheidungsfindung ist aufgrund von Art. 22 Abs. 1 DSGVO verboten.[19] Dadurch, dass eine ausschließlich automatisierte Entscheidungsfindung ohnehin grundsätzlich ausgeschlossen ist und auch etwaige Ausnahmen nach Art. 22 Abs. 2 DSGVO für den Untersuchungsgegenstand der Arbeit nicht in Betracht kommen[20], liegt somit niemals ein rein durch ein algorithmisches System vorgenommenes Ergebnis vor. Die Entscheidung trifft final der Mensch, sodass eine Behandlung i. S. d. § 3 Abs. 1 AGG vorliegt.

Wimmer zufolge kann eine weniger günstige Behandlung bereits in der Entscheidungsvorbereitung durch algorithmische Systeme liegen.[21] Nach dem bereits erwähnten Urteil des EuGH vom 23.4.2020 [22] wird der Begriff „Bedingungen für den Zugang zu [einer] Erwerbstätigkeit" i. S. v. Art. 3 Abs. 1 lit. a. der Richtlinie 2000/78 weit ausgelegt. Werden Bedingungen mit der Einstellungspolitik in Verbindung gebracht, könne darin bereits eine weniger günstige Behandlung, also auch eine Benachteiligung liegen. Wenn ein algorithmisches Entscheidungssystem im Bewerbungsprozess eingesetzt werde, werde es mithin Teil der Einstellungspolitik. Eine weniger günstige Behandlung liege demnach vor.

Selbst wenn man der Argumentation von *Wimmer* folgt, ist entscheidend, dass die spürbare tatsächliche Benachteiligung erst eintritt, wenn die Arbeitgeberin anknüpfend an das Ergebnis des Systems ihre Auswahlentscheidung trifft. In der Praxis wird die Entscheidung des Menschen Anknüpfungspunkt für die Benachteiligung sein, sodass die Frage, ob ein benachteiligendes Ergebnis eines algorithmischen Systems eine Behandlung i. S. d. § 3 Abs. 1 AGG ist, nicht entschieden werden muss. Hinzu

---

[18] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 356.

[19] S. Kapitel 6 D.II. (S. 207).

[20] S. Kapitel 6 D.IV.5. (S. 224).

[21] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 357.

[22] EuGH, 23.4.2020 – C-507/18, *Associazione Avvocatura per i diritti LGBTI ./. Rete Lenford.*

kommt, dass die Besonderheit des Sachverhalts, den der EuGH zu entscheiden hatte, darin lag, dass die Vereinigung von Rechtsanwältinnen befugt war, gegen die Benachteiligung einer Personengruppe zu klagen, obwohl es keine Geschädigte gab.[23] Ein derartiges Verbandsklagerecht gibt es im nationalen Recht (noch) nicht.[24]

b) Erweiterung des Anwendungsbereichs des § 1 AGG de lege ferenda

Die Bundesbeauftragte für Antidiskriminierung hat jüngst vorgeschlagen, „Handeln durch automatisierte Entscheidungssysteme (...) als Benachteiligungstatbestand in § 3 AGG" aufzunehmen.[25] Damit schlägt sie aus einer gesetzgeberischen Perspektive in eine ähnliche Kerbe wie *Wimmer*. Zu kritisieren ist indes, dass der Vorschlag der Antidiskriminierungsstelle nicht mit dem erfolgsbezogenen Regelungsansatz des AGG in Einklang zu bringen ist. Das AGG schützt vor Diskriminierung aufgrund bestimmter Tatbestände, z. B. des Geschlechts. Das tut es auch beim Einsatz von KI auch schon *de lege lata*. Würde man den Einsatz von KI als eigenständigen Benachteiligungstatbestand einfügen, wäre dieser nicht erfolgsbezogen, sondern würde sich auf das der Entscheidung zu Grunde liegende Verfahren beziehen. Das würde faktisch wohl zu einem weitgehenden Ausschluss des Einsatzes von KI-Entscheidungssystemen führen. Sinnvoller ist es, zu untersuchen, wann eine durch KI unterstützte Entscheidung nach Maßgabe der bestehenden erfolgsbezogenen Kriterien tatsächlich zu einer Diskriminierung führt. Eines neuen Benachteiligungstatbestands bedarf es dafür nicht.

Spiecker gen. Döhmann und *Towfigh* haben im Auftrag der Antidiskriminierungsstelle des Bundes ein Rechtsgutachten mit dem Titel „Automatisch benachteiligt" erstellt, in dem sie untersuchen, ob das AGG in

---

[23] Zur opferlosen Diskriminierung s. *Sesing/Tschech*, MMR 2022, 24, 27.

[24] Für ein echtes Verbandsklagerecht im AGG s. etwa *Lauscher/Legner*, ZfDR 2022, 367, 389; *Herberger*, RdA 2022, 220; *Meller-Hannich/Hundertmark*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 189, 198; *Ponti/Tuchtfeld*, ZRP 2018, 139; s. dazu auch: *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 79 ff.

[25] *Unabhängige Bundesbeauftragte für Antidiskriminierung*, Vielfalt, Respekt, Antidiskriminierung, 2023, S. 3.

seiner bestehenden Form hinreichend vor Diskriminierung durch algorithmische Entscheidungssysteme schützt. Unter anderem schlagen sie vor, § 1 AGG um das Diskriminierungsmerkmal „Benachteiligung aufgrund von Beziehungen" zu erweitern.[26] Diese Erweiterung sei notwendig, um Diskriminierungen zu erfassen, die sich aus Beziehungen ergäben, die nur auf statistischer Korrelation beruhen würden.[27] Zur weiteren Erklärung verwenden *Spiecker gen. Döhmann* und *Towfigh* den Begriff der „Gruppenbildung".[28] Faktisch ergebe sich die Diskriminierung dadurch, dass es im System bestimmte implizite „Gruppen" gebe, denen betroffene Personen zugeordnet würden. Ein mögliches Beispiel für eine solche Gruppe sind Personen mit einer besonderen Teamfähigkeit.

Nach Auffassung von *Spiecker gen. Döhmann* und *Towfigh* soll eine Benachteiligung i. S. d. insoweit zu ändernden § 1 AGG vorliegen, wenn sich die Diskriminierung „aus einer Beziehung ergibt, die nur auf statistischer Korrelation beruht".[29] Das ist wohl so zu verstehen, dass die Benachteiligung voraussetzt, dass eine Person fälschlicherweise aufgrund statistischer Korrelation einer bestimmten Gruppe zugeordnet wird und dadurch benachteiligt wird, obwohl sie der Gruppe in Wirklichkeit gar nicht angehört. Dabei soll es nach *Spiecker gen. Döhmann* und *Towfigh* nicht darauf ankommen, ob die Gruppenzugehörigkeit in Zusammenhang mit einem der bereits bestehenden Merkmale des § 1 AGG steht. Auch eine nach dem aktuellen AGG „erlaubte" Benachteiligung – z. B. einer „nicht teamfähigen" Person – würde nach dem Änderungsvorschlag zu einem AGG-Verstoß führen, wenn sie auf falscher statistischer Korrelation beruht: Wenn eine Person tatsächlich teamfähig ist, soll § 1 AGG in der geänderten Fassung betroffen sein, wenn das Entscheidungssystem sie zu Unrecht als „nicht teamfähig" ansieht.

Der Vorschlag von *Spiecker gen. Döhmann* und *Towfigh* ist aus drei Gründen nicht überzeugend. Erstens fehlt der „Benachteiligung aufgrund von Beziehungen" der materielle Charakter der bisher in § 1 AGG genannten

---

[26] *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 72 f.
[27] *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 73.
[28] *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 72.
[29] *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 73.

Gründe. Der AGG-Verstoß ergibt sich dabei nicht aus dem Entscheidungsgrund selbst, sondern daraus, dass dieser durch falsche statistische Korrelation entstanden ist. Damit passt der Vorschlag nicht zur Konzeption des § 1 AGG, da er nicht den Entscheidungsgrund, sondern das Entscheidungsverfahren betrifft.

Zweitens steht der Vorschlag in Konflikt mit § 7 Abs. 1 Hs. 2 AGG. Nach § 7 Abs. 1 Hs. 2 AGG liegt ein AGG-Verstoß auch dann vor, wenn die Entscheiderin das Vorliegen eines in § 1 AGG genannten Grundes bei der Benachteiligung nur annimmt. Es ist also irrelevant, ob eine Person tatsächlich wegen einer Gruppenzugehörigkeit nach § 1 AGG benachteiligt wurde. Entscheidend ist, dass die Entscheiderin deswegen benachteiligen wollte. Bei der von *Spiecker gen. Döhmann* und *Towfigh* vorgeschlagenen Benachteiligung wegen Beziehungen soll es dem widersprechend aber gerade darauf ankommen, dass eine Person einer – nicht unter § 1 AGG fallenden – Gruppe tatsächlich angehört. Der Verstoß setzt die fälschliche Zuordnung aufgrund statistischer Korrelation voraus. Man kann diese nicht gem. § 7 Abs. 1 Hs. 2 AGG „nur" annehmen. Hierin zeigt sich, dass ein Diskriminierungstatbestand, der nicht an den Entscheidungsgrund selbst anknüpft, nicht zur Systematik des bestehenden AGG passt.

Drittens stellt sich die Frage, wie man eine fehlerhafte statistische Korrelation nachweist. Es wird typischerweise schwierig sein, herauszufinden, welche Korrelationen das algorithmische System vorgenommen hat. Einzelne Entscheidungsfaktoren lassen sich bei komplexen algorithmischen Systemen aus technischen Gründen wohl nur selten isolieren. Ebenso lässt es sich oft kaum nachweisen, dass eine Gruppenzugehörigkeit vom System zu Unrecht angenommen wurde. Das gilt insbesondere bei schillernden Begriffen, wie etwa der als Beispiel erwähnten Teamfähigkeit.

c) Kausalität

Die Benachteiligung muss *wegen* eines in § 1 AGG genannten Merkmals erfolgen; ein Merkmal nach § 1 AGG muss kausal für die Benachteiligung

sein.[30] Häufig erfolgt die Benachteiligung nicht nur aufgrund eines Merkmals, sondern aufgrund von mehreren Merkmalen, unter denen sich auch zulässige Merkmale befinden. Ein solches sog. Motivbündel genügt nach der Rechtsprechung, um eine Benachteiligung anzunehmen. [31] Maschinell lernende Systeme werden mit vielen Daten trainiert, sodass davon auszugehen ist, dass die Benachteiligung häufig nicht nur auf einem Merkmal beruhen wird.[32]

Basiert das eingesetzte System etwa auf einem künstlichen neuronalen Netz[33], liegt ein Verstoß gegen § 7 Abs. 1 AGG vor, wenn nur einer der Vielzahl an (Millionen) Parametern allein oder mit anderen Parametern gemeinsam unmittelbar oder mittelbar an ein geschütztes Merkmal nach § 1 AGG anknüpft.[34] Die Kausalität entfällt auch nicht deshalb, weil der Mensch ggf. keine Kenntnis der diskriminierenden Parameter[35] hat. Vielmehr macht sich der Mensch bei einem entscheidungsunterstützenden Einsatz das Ergebnis des Systems zu eigen, indem er das Ergebnis mit in seine finale Entscheidung einbezieht.[36]

2. Mittelbare Benachteiligung

Eine mittelbare Benachteiligung liegt vor, wenn dem Anschein nach neutrale Vorschriften, Kriterien oder Verfahren Personen wegen eines in § 1 AGG genannten Grundes gegenüber anderen Personen in besonderer Weise benachteiligen können (§ 3 Abs. 2 AGG). Wie bereits erklärt worden ist, können algorithmische Entscheidungen benachteiligen, wenn vermeintlich neutrale Merkmale wie der Wohnort oder die Betriebszugehörigkeit[37] durch

---

[30] Statt vieler: BeckOK Arbeitsrecht/*Roloff*, § 3 AGG Rn. 12; Däubler/Beck/*Beck*, § 22 AGG Rn. 56

[31] BAG, 22.10.2015 – 8 AZR 384/14, NZA 2016, 625, Rn. 25; ErfK/*Schlachter*, § 7 AGG Rn. 3.

[32] *Freyler*, NZA 2020, 284, 287; *Höpfner/Daum*, ZfA 2021, 467, 492; *Lewinski/Barros Fritz*, NZA 2018, 620, 622.

[33] Kapitel 1 C.II. (S. 17).

[34] *Höpfner/Daum*, ZfA 2021, 467, 493.

[35] *Dies.*, ZfA 2021, 467, 493 f.

[36] *Dies.*, ZfA 2021, 467, 494.

[37] *Dzida/Groh*, NJW 2018, 1917, 1919.

das Training des maschinell lernenden Systems mit anderen Merkmalen verknüpft werden. Bei solchen Systemen wird die mittelbare Benachteiligung die relevanteste Form der Benachteiligung sein.[38] Das liegt daran, dass die verwendeten Kriterien, die dem System zugrunde liegen, in aller Regel neutrale Kriterien sind, die geschützte Gruppen benachteiligen können.[39] Wie bereits erläutert worden ist, kann das System Kriterien als Grundlage für eine Entscheidung heranziehen, durch die mittelbar eine bestimmte Personengruppe diskriminiert wird. Korreliert z. B. das Merkmal „Wohnort außerhalb der Stadt" mit Kündigungsabsichten, wird die Personengruppe benachteiligt, die außerhalb der Stadt wohnt.[40]

Spiecker gen. Döhmann und *Towfigh* schlagen vor, algorithmische Entscheidungssysteme in die Legaldefinition des § 3 Abs. 2 AGG aufzunehmen, damit deutlich werde, dass ein solche System auch als „Verfahren" i. S. d. § 3 Abs. 2 AGG gelten würde.[41] Diese Änderung ist vor dem Hintergrund der obigen Auslegung des Art. 3 Abs. 2 AGG nicht zwingend notwendig, führt aber zu mehr Rechtssicherheit und ist daher zu begrüßen.

Für das Merkmal der Kausalität gelten die gleichen Erwägungen wie bereits oben ausgeführt.[42]

III. Rechtfertigung

1. Rechtfertigung einer unmittelbaren Benachteiligung

a) Gem. §§ 8-10 AGG

Eine unmittelbare Benachteiligung kann gem. §§ 8-10 AGG gerechtfertigt sein, etwa wenn eine unterschiedliche Behandlung wegen beruflicher Anforderungen, wegen der Religion oder Weltanschauung oder wegen des Alters erforderlich ist. Wenn algorithmische Systeme zur Vorauswahl

---

[38] *Hacker*, CMLR 2018, 1143, 1154.
[39] *Ders.*, CMLR 2018, 1143, 1154.
[40] S. Kapitel 8 B.II. (S. 289); dazu auch: *ders.*, CMLR 2018, 1143, 1154.
[41] *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 73.
[42] Kapitel 9 A.II.1.b) (S. 298).

unterstützend eingesetzt werden, sind die Anforderungen an die Rechtfertigung nicht anders, als wenn ausschließlich ein Mensch die Vorauswahl trifft.[43] Je nach Einzelfall kann ggf. eine Benachteiligung aufgrund eines in § 1 AGG genannten Merkmals gerechtfertigt werden.[44]

b) Gem. § 5 AGG

Die Arbeitgeberin kann gem. § 5 AGG durch geeignete und angemessene Maßnahmen bestehende Nachteile wegen eines in § 1 genannten Grundes verhindern oder ausgleichen. § 5 AGG ist ein Rechtfertigungsgrund, der erst in Betracht kommt, wenn die §§ 8-10 AGG sowie § 20 AGG nicht erfüllt sind.[45] Der Rechtfertigungsgrund nach § 20 AGG wird regelmäßig nicht erfüllt sein, wenn algorithmische Systeme eingesetzt werden. Anders ist es bei § 5 AGG: Der Einsatz eines algorithmischen Systems kann eine positive Maßnahme nach § 5 AGG sein: Das Recruiting-Software-Unternehmen *Entelo* hatte etwa ein System entwickelt, das Bewerberinnen speziell nach geschützten Merkmalen sortiert hat, weil die Arbeitgeberin das Geschlechtergleichgewicht in ihrem Ingenieurteam verbessern wollte.[46]

2. Rechtfertigung einer mittelbaren Benachteiligung

Eine mittelbare Benachteiligung kann bereits auf Tatbestandsebene gerechtfertigt sein, wenn die betreffenden Vorschriften, Kriterien oder Verfahren durch ein rechtmäßiges Ziel sachlich gerechtfertigt und die Mittel zur Erreichung dieses Ziels angemessen und erforderlich sind (§ 3 Abs. 1 Hs. 2 AGG).[47]

---

[43] *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 54.

[44] Ausführlich dazu s. *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 381 ff.

[45] HK-ArbR/*Turba/Klapp*, § 5 AGG Rn. 1.

[46] *Rosenblat/Wikelius/boyd u.a.*, SSRN Journal 2014, 2; Hoeren/Sieber/Holznagel, MultimediaR-Hdb/*Straker*, Teil 15.6 Rn. 57.

[47] S. dazu auch die Ausführungen von *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 55.

a) Rechtmäßiges Ziel

Ein Ziel ist rechtmäßig, wenn es nicht seinerseits diskriminierend und auch im Übrigen legal ist.[48] Arbeitgeberinnen möchten Bewerbungsverfahren mit dem Ziel durchführen, die am besten geeignete Kandidatin zu finden. Das ist ein grundsätzlich rechtmäßiges Ziel.[49] Gleiches gilt auch für den Fall, wenn die Arbeitgeberin die geeignete Kandidatin für eine Beförderung auswählen möchte. Schließlich liegt auch ein an sich rechtmäßiges Ziel vor, wenn die Arbeitgeberin herausfinden möchte, ob eine Arbeitnehmerin plant, im Unternehmen zu bleiben, oder beabsichtigt, zu kündigen.

b) Verhältnismäßigkeit

Die Personalauswahl durch das mittelbar benachteiligende maschinell lernende System muss geeignet, erforderlich und angemessen, also verhältnismäßig sein.[50]

aa) Geeignetheit

Damit die mittelbare Benachteiligung auf Tatbestandsebene ausgeschlossen wird, muss die Anknüpfung an ein neutrales, tatsächlich aber benachteiligendes Merkmal geeignet sein, die am besten geeignete Kandidatin zu finden. Wird ein neuronales Netz eingesetzt, um ein maschinell lernendes System zu generieren, wird allerdings nicht nachvollziehbar sein, wie genau das Ergebnis zustande gekommen ist[51]: Bei einem Sprachmodell von *Microsoft* wurden 530 Milliarden Parameter verwendet. [52] Bei derart komplexen Systemen wird man nicht hinreichend offenlegen können, welche Parameter und Gewichtungen für die konkrete Entscheidung ausschlaggebend waren. Es ist daher mitunter uneindeutig, inwiefern die Entscheidung mithilfe des

---

[48] BeckOK Arbeitsrecht/*Roloff*, § 3 AGG Rn. 18 ff.; ErfK/*Schlachter*, § 3 AGG Rn. 13; *Dzida/Groh*, NJW 2018, 1917, 1920.

[49] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 381; vgl. BAG, nach dem die bestmögliche Verrichtung der Tätigkeit ein rechtmäßiges Ziel darstellt: BAG, 29.6.2017 – 8 AZR 402/15, NZA 2018, 33, 39 Rn. 62; BAG, 15.12.2016 – 8 AZR 454/15, NZA 2017, 715, 720 Rn. 45.

[50] BAG, 29.6.2017 – 8 AZR 402/15, NZA 2018, 33, 39 Rn. 61.

[51] S. dazu bereits Kapitel 3 C (S. 36).

[52]Kapitel 1 C.II. (S. 17).

maschinell lernenden Systems geeignet ist, die passende Kandidatin herauszufiltern.[53]

Die Arbeitgeberin trägt die Beweislast dafür, dass rechtfertigende Tatsachen vorliegen.[54] Wenn es allerdings je nach verwendetem Lernverfahren nicht möglich ist, die verwendeten Kriterien offenzulegen und auf ihre Eignung hin zu überprüfen, ist eine Rechtfertigung praktisch ausgeschlossen.[55] Ein solches Ergebnis lässt aber laut *Lauscher* und *Legner* außer Betracht, dass das Tatbestandsmerkmal der mittelbaren Benachteiligung sehr weit gefasst sei und die Rechtfertigung bereits im Tatbestand verankert worden sei.[56] Ausreichend müsse daher sein, dass die Arbeitgeberin für das Merkmal der Geeignetheit nachweist, dass das maschinell lernende System entsprechende Test- und Validierungsverfahren durchlaufen habe.[57] Außerdem solle die Arbeitgeberin offenlegen, wie sie ihre Trainingsdaten ausgewählt habe. Schließlich hängt die Geeignetheit eines Modells auch maßgeblich von der Qualität der verwendeten Trainingsdaten ab.[58] Zukünftig wird ohnehin Art. 10 Abs. 5 KI-VO-KOM greifen, der Anforderungen an Trainingsdaten aufstellt.[59] Bei den untersuchten algorithmischen Systemen handelt es sich um Hochrisiko-KI-Systeme, für die Art. 10 Abs. 5 KI-VO-KOM zukünftig gelten wird.[60]

Diese Argumentation überzeugt insbesondere vor dem Hintergrund, dass man die Geeignetheit der Entscheidung einer Personalerin, die eine Auswahlentscheidung trifft, auch nicht grundsätzlich infrage stellt, weil man ggf. nicht alle Kriterien, die mit in die Entscheidung einfließen, offenlegen kann.

---

[53] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 384.

[54] BAG, 14.12.2016 – 7 AZR 688/14, NZA 2017, 715, 719; ErfK/*Schlachter*, § 3 AGG Rn. 9.

[55] *Lauscher/Legner*, ZfDR 2022, 367, 377.

[56] *Dies.*, ZfDR 2022, 367, 376 f.

[57] *Dies.*, ZfDR 2022, 367, 377; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 384 f.

[58] S. dazu bereits: Kapitel 6 C.IV.2.b)aa) (S. 176).

[59] Kapitel 10 B.I. (S. 345).

[60] Kapitel 5 A.IV.5. (S. 82).

Kann die Arbeitgeberin somit darlegen und beweisen, welche Test- und Validierungsverfahren das algorithmische System durchlaufen hat und ob die Trainingsdaten qualitativ hochwertig waren, d. h. in den überwiegenden Fällen die Anforderungen nach Art. 10 Abs. 5 KI-VO-KOM gewahrt sind, ist von der Geeignetheit des Systems auszugehen.

bb) Erforderlichkeit

Der Einsatz des maschinell lernenden Systems ist erforderlich, wenn es ihm gegenüber kein gleich geeignetes, milderes Mittel gibt. Ein Mittel ist milder, wenn es die legitimen Interessen der Person weniger stark beeinträchtigt.[61] Wenn es um den Einsatz algorithmischer Systeme bei arbeitsrechtlichen Auswahlentscheidungen geht, ist insbesondere das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG beeinträchtigt.

Als mildere Mittel könnte man zunächst herkömmliche Bewerbungsabläufe wie etwa das Auswahlgespräch mit einer Personalerin einordnen. Wird ein algorithmisches System im bestehenden Arbeitsverhältnis eingesetzt, um potenzielle Kandidatinnen zur Beförderung vorauszuwählen, könnte man etwa Gespräche mit Personalerinnen als mildere Mittel in Betracht ziehen. Allerdings sind diese Methoden nicht zwingend milder als der unterstützende Einsatz eines algorithmischen Systems: Wie im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO bereits erläutert worden ist, können bei Verfahren durch algorithmische Systeme die Antworten in der Regel mehrmals aufgenommen bzw. eingetippt werden – es entsteht keine vergleichbare Drucksituation wie in einem persönlichen Gespräch mit der Person, die eine Entscheidung über das Arbeitsverhältnis trifft.[62] Hinzu kommt, dass ein herkömmliches Verfahren gegenüber einem algorithmischen System nicht unbedingt gleich geeignet ist: Wie auch bei Art. 6 Abs. 1 S. 1 lit. b DSGVO sollte man sowohl die qualitative als auch die quantitative Ebene bei der Frage nach der gleichen Eignung berücksichtigen. Zum einen muss gewährleistet sein, dass die Entscheidung von hoher Qualität ist. Ein maschinell lernendes System muss hinreichend auf etwaige Fehlertypen getestet worden sein, sodass etwa keine

[61] BeckOK Arbeitsrecht/*Roloff*, § 3 AGG Rn. 21.
[62] S. Kapitel 6 C.IV.2.c)aa) (S. 178).

Korrelationen zwischen Merkmalen hergestellt werden, die sich nicht gegenseitig bedingen. Z. B. darf – wie bereits ausgeführt worden ist – ein außerhalb des Stadtzentrums liegender Wohnort nicht dazu führen, dass Kandidatinnen bei einer Stelle, die im Stadtzentrum zu besetzen ist, benachteiligt werden.[63] Zum anderen muss das jeweilige Verfahren für die Menge an Daten gleich geeignet sein. Bei einer großen Anzahl auszuwertender Daten wird das algorithmische System in quantitativer Hinsicht sogar besser geeignet sein als die menschliche Entscheidungsstruktur.[64]

Außerdem könnte man als milderes Mittel gegenüber dem mittelbar benachteiligenden System erwägen, ein maschinell lernendes System einzusetzen, das mit weniger Entscheidungskriterien arbeitet. Womöglich lassen sich Benachteiligungen von vornherein verhindern. Allerdings ist es schwierig herauszufinden, wie einzelne Kriterien eine Entscheidung eines solchen Systems beeinflussen werden. Man kann somit nicht eindeutig feststellen, ob ein maschinell lernendes System, welches mit weniger Kriterien arbeitet, ein gleich geeignetes, milderes Mittel ist gegenüber dem System, welches auf der Grundlage vieler Kriterien zu einer Entscheidung kommt.[65]

cc) Angemessenheit

Der Einsatz des mittelbar benachteiligenden algorithmischen Systems muss für das angestrebte Ziel angemessen sein. Das bedeutet, dass der Einsatz des Systems nicht zu einer übermäßigen Beeinträchtigung der legitimen Interessen der Personen führen darf, die wegen eines in § 1 AGG genannten Grundes mittelbar benachteiligt werden.[66] Der Einsatz des algorithmischen Systems darf daher nicht dazu führen, dass übermäßig das allgemeine Persönlichkeitsrecht der betroffenen Personen beeinträchtigt wird. Im Rahmen der Angemessenheit sind nicht dieselben Erwägungen, die bei Art. 6 Abs. 1 S. 1 lit. b DSGVO eine Rolle spielen[67], heranzuziehen. Es geht bei

---

[63] S. Kapitel 8 B.II. (S. 289).

[64] S. dazu Kapitel 3 B. (S. 35).

[65] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 386.

[66] Vgl. BeckOK Arbeitsrecht/*Roloff*, § 3 AGG Rn. 21; BAG, 15.12.2016 – 8 AZR 454/15, NZA 2017, 715, Rn. 39.

[67] Kapitel 6 C.IV.2.d) (S. 182).

Angemessenheit i. S. d. § 3 Abs. 1 Hs. 2 AGG nicht darum, ob die Verarbeitung grundsätzlich angemessen ist, sondern darum, ob der *Einsatz des mittelbar benachteiligenden Verfahrens* angemessen ist.

Auch bei menschlichen Entscheidungen können Personen mittelbar benachteiligt werden: Jedenfalls ist eine rein menschliche Entscheidung nicht unbedingt frei von Vorurteilen, sodass das Persönlichkeitsrecht ebenfalls beeinträchtigt wird.[68] Das allgemeine Persönlichkeitsrecht würde aber weniger stark beeinträchtigt werden, wenn ein maschinell lernendes System zu weniger mittelbar benachteiligenden Ergebnissen kommt. Das bedeutet im Umkehrschluss, dass die Arbeitgeberin ein solches System einsetzen müsste, welches aufgrund eines qualitativ hochwertigen Trainingsdatensatzes trainiert wurde, sodass auch mittelbare Benachteiligungen möglichst nicht vorkommen.[69] Ein solches Trainingsdatenset als Grundlage für das Training zu nehmen, wird allerdings mit erheblichen Kosten verbunden sein.[70] *Hacker* schlägt daher vor, dass nur unverhältnismäßige Kosten die verantwortliche Person davon abhalten sollten, ein solches Trainingsdatenset zu verwenden.[71] Der Begriff Unverhältnismäßigkeit müsse im Kontext der Bedeutung der Folgen der Entscheidung des algorithmischen Systems ausgelegt werden: Je eher Grundrechte beeinträchtigt werden würden, desto höher müssten die Kosten sein, die der Entscheidungsträger aufwenden müsste.[72] Wird ein algorithmisches System zur Bewerberinnenvorauswahl oder Vorauswahl von potenziell zu befördernden Arbeitnehmerinnen eingesetzt, sind Grundrechte der Person womöglich beeinträchtigt: Jedenfalls ist die informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG betroffen, weil personenbezogene Daten verarbeitet werden.[73]

Ist es nicht möglich, ein qualitativ höherwertigeres Trainingsdatenset zu verwenden, etwa weil ein solches nicht verfügbar ist oder die Kosten unverhältnismäßig sind, ist der Einsatz des algorithmischen Systems trotzdem

---

[68] *Hacker*, CMLR 2018, 1143, 1162; *Lauscher/Legner*, ZfDR 2022, 367, 377.
[69] S. dazu auch: *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 77.
[70] *Hacker*, CMLR 2018, 1143, 1162.
[71] *Ders.*, CMLR 2018, 1143, 1162.
[72] *Ders.*, CMLR 2018, 1143, 1162.
[73] S. dazu bereits unter: Kapitel 5 B.I. (S. 86).

angemessen, wenn nachgewiesen werden kann, dass das System signifikant und nachweislich weniger voreingenommen zu Ergebnissen kommt als andere (nicht algorithmische) Verfahren.[74] Wenn diese Voraussetzung erfüllt ist, führt der Einsatz des algorithmischen Systems in der Summe zu weniger Benachteiligungen. Es wäre somit widersprüchlich, wenn das AGG den Einsatz des Systems verbieten würde. An den Nachweis, dass das System tatsächlich zu weniger Benachteiligungen führt, sind aber strenge Anforderungen zu stellen. Im Regelfall wird eine empirischen und wissenschaftlichen Anforderungen genügende Untersuchung des tatsächlichen Einsatzszenarios erforderlich sein.

dd) Zwischenergebnis

Die mittelbare Benachteiligung, die durch den Einsatz algorithmischer Systeme hervorgerufen wird, kann im Einzelfall bereits auf Tatbestandsebene ausgeschlossen werden, wenn die Voraussetzungen nach § 3 Abs. 2 AGG erfüllt sind. Grundsätzlich liegt ein legitimes Ziel vor, wenn die Arbeitgeberin die am besten geeignete Kandidatin für eine Stelle finden möchte oder herausfinden will, ob eine Arbeitnehmerin weiterhin beabsichtigt, im Unternehmen zu bleiben. Im Rahmen der Erforderlichkeit kann auf die Erwägungen, die bei Art. 6 Abs. 1 S. 1 lit. b DSGVO angeführt worden sind, zurückgegriffen werden.[75] Demnach muss das algorithmische System sowohl in qualitativer als auch in quantitativer Hinsicht geeignet sein: Die Entscheidung muss von hoher Qualität sein, d. h., es dürfen etwa keine unzutreffenden Korrelationen zwischen Informationen hergestellt werden. Auch in quantitativer Hinsicht, d. h. für die Menge an Daten, die verarbeitet werden, muss das algorithmische System geeignet sein. Im Rahmen der Angemessenheit ist zu berücksichtigen, ob die Arbeitgeberin die Kosten für ein qualitativ höherwertigeres und somit weniger zu Benachteiligungen führendes Trainingsdatenset aufwenden kann. Alternativ kann die Arbeitgeberin nachweisen, dass das eingesetzte System signifikant und

---

[74] *Hacker*, CMLR 2018, 1143, 1162.

[75] Kapitel 6 C.IV.2.c) (S. 178).

nachweislich weniger voreingenommen zu Ergebnissen kommt als andere (nicht algorithmische) Verfahren.[76]

B. Haftung bei Verstößen gegen das Benachteiligungsverbot

I. Schadensersatz nach § 15 Abs. 1 S. 1 AGG

Gem. § 15 Abs. 1 S. 1 AGG ist die Arbeitgeberin bei einem Verstoß gegen das Benachteiligungsverbot dazu verpflichtet, den hierdurch entstandenen Schaden zu ersetzen. Der Schadensersatzanspruch setzt nach § 15 Abs. 1 S. 2 AGG ein Vertretenmüssen der Arbeitgeberin voraus: Die Rechtsfolge des § 15 Abs. 1 S. 1 AGG gilt nicht, wenn die Arbeitgeberin die Pflichtverletzung nicht zu vertreten hat. Außen vor gelassen wird an dieser Stelle, dass die Voraussetzung des Vertretenmüssens in der Literatur überwiegend als richtlinienwidrig eingestuft wird.[77] Dem ist insbesondere deshalb zuzustimmen, weil ein Verschuldenserfordernis den effektiven Schutz vor Diskriminierungen relativieren würde.[78] Sieht man aus diesem Grund von dem Merkmal des Vertretenmüssens ab, sind die nachfolgenden Ausführungen zum Vertretenmüssen nicht zu berücksichtigen.

1. Vertretenmüssen der Arbeitgeberin

Das Vertretenmüssen richtet sich nach den §§ 276 ff. BGB.[79] Die Arbeitgeberin hat nach § 276 Abs. 1 BGB Vorsatz und Fahrlässigkeit zu vertreten. Fahrlässig handelt nach § 276 Abs. 2 BGB, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Wurde ein maschinell lernendes System fehlerhaft programmiert, mit unzureichenden Daten trainiert oder entspricht es nicht den geltenden technischen Standards, kann darin eine

---

[76] *Hacker*, CMLR 2018, 1143, 1162.

[77] S. etwa: BeckOK Arbeitsrecht/*Roloff*, § 15 AGG Rn. 2; *Benecke*, in: Brose/Greiner/Rolfs u.a. (Hrsg.), Grundlagen des Arbeits- und Sozialrechts, 2021, S. 73, 74 ff.; ErfK/*Schlachter*, § 15 AGG Rn. 1.

[78] EuGH, 8.11.1990 – C-177/88, *Dekker*, NZA 1991, 171, 172 Rn. 24.

[79] ErfK/*Schlachter*, § 15 AGG Rn. 6; *Benecke*, in: Brose/Greiner/Rolfs u.a. (Hrsg.), Grundlagen des Arbeits- und Sozialrechts, 2021, S. 73, 74.

Sorgfaltspflichtverletzung liegen.[80] Diese Gründe sind aber in der Regel nicht auf die Arbeitgeberin zurückzuführen, sondern auf das Verhalten der Programmiererin des algorithmischen Systems. Es könnte sich z. B. folgender Fall abspielen: Ein maschinell lernendes System wird zur Auswahl von Bewerberinnen trainiert. Eine Arbeitgeberin setzt das System in einem konkreten Bewerbungsprozess ein. Aufgrund fehlerhafter Korrelationen und der entsprechend vorgenommenen Gewichtungen des maschinell lernenden Systems wurden Bewerberinnen asiatischer Herkunft vom System nicht als solche identifiziert und deshalb nicht als potenzielle Arbeitnehmerinnen vorgeschlagen. Das maschinell lernende System hätte Bewerberinnen mit asiatischer Herkunft erkannt, wenn alle technischen Standards eingehalten worden wären. Indem die Bewerberinnen asiatischer Herkunft nicht berücksichtigt werden, werden sie jedenfalls mittelbar nach § 3 Abs. 2 AGG benachteiligt. Hat die Arbeitgeberin den Verstoß gegen das Benachteiligungsverbot gem. § 15 Abs. 1 S. 1 AGG zu vertreten? Die Benachteiligung resultiert hier auch aus den fehlerhaften Korrelationen oder den vorgenommenen Gewichtungen des Systems. Der Fehler liegt also im „Inneren" des Systems und lässt sich nicht auf einen leichter zu erkennenden Fehler wie etwa unvollständige Trainingsdaten zurückführen. Hat die Arbeitgeberin den Verstoß gegen das Benachteiligungsverbot auch zu vertreten, wenn es um einen derartigen Fehler geht? Das wiederum hängt mit der Frage zusammen, welches *Wissen* die Arbeitgeberin über das eingesetzte System haben muss.

a) Eigenes Verschulden der Arbeitgeberin – Grundsätze der Wissenszurechnung

Kuntz untersucht, inwiefern die Grundsätze der Wissenszurechnung beim Einsatz maschinell lernender Systeme herangezogen werden können, um Daten und Verarbeitungsvorgänge der juristischen oder natürlichen Person zuzurechnen.[81] Ausgangspunkt für die Dogmatik der Wissenszurechnung ist § 166 BGB. Nach § 166 Abs. 1 BGB ist der Vertretenen die Kenntnis sowie das Kennenmüssen ihrer Vertreterin zuzurechnen. § 166 BGB ist mithin auch eine

---

[80] Vgl. *Burchardi*, EuZW 2022, 685, 686.

[81] *Kuntz*, ZfPW 2022, 178, 179; s. umfassend dazu auch: *Hacker*, RW 2018, 243; *Linke*, Digitale Wissensorganisation, 2021.

Zurechnungsnorm, knüpft nur anders als § 278 BGB nicht an das *Verschulden*, sondern an das *Wissen* an. Der Anknüpfungspunkt der beiden Normen ist somit unterschiedlich. Wenn eine juristische oder natürliche Person nach den Grundsätzen der Wissenszurechnung von einem bestimmten Aspekt weiß, kann es sein, dass sie die im Verkehr erforderliche Sorgfalt außer Acht gelassen hat und ihr deshalb ein Verschulden zur Last fällt. Wissen und Verschulden liegen aber keineswegs immer gleichgleichermaßen vor.

Der BGH differenziert zwischen den Wissensvertreterinnen und der Pflicht zur Wissensorganisation.[82] Der Geschäftsherrin wird analog § 166 Abs. 1 BGB das Wissen von Hilfspersonen zugerechnet, derer sie sich „wie eine[r] Vertreter[in]“ bedient.[83] Eine solche Wissensvertreterin ist eine Person, die im Rechtsverkehr als Repräsentantin der Geschäftsherrin bestimmte Aufgaben in eigener Verantwortung erledigt und angefallene Informationen wahrnimmt und sie ggf. weiterleitet.[84] Zudem ist Wissen zuzurechnen, „wenn es bei ordnungsgerechter Organisation aktenmäßig festzuhalten, weiterzugeben und abzufragen ist“[85].

Inwiefern ein maschinell lernendes System selbst Wissensvertreterin sein kann, lässt *Kuntz* dahinstehen.[86] Vielmehr erarbeitet er, in welcher Weise sich Grundsätze zur Speicherung und dem Abruf von Daten auf KI übertragen lassen.[87] Problematisch sei, dass bei KI die Menge der erfassten Daten erheblich ansteige und die vom BGH aufgestellte Prämisse, nach der die Wissenszurechnung „nicht zu einer Fiktion entarten“ dürfe, „die juristische Personen [...] weit über jede menschliche Fähigkeit hinaus belastet“[88], relevant werde.[89] Die von der KI erfasste Menge an Daten könne von einem Menschen unmöglich erfasst werden; jedenfalls gehe die erfasste Datenmenge weit über klassische Datenspeicher und das „Aktenwissen“ hinaus. Außerdem sei bei

---

[82] *Kuntz*, ZfPW 2022, 178, 180.

[83] BGH, 10.2.1971 – VIII ZR 182/69, NJW 1971, 1702, 1703; *Linke*, RDi 2021, 400, 402.

[84] *Kuntz*, ZfPW 2022, 178, 180.

[85] *Ders.*, ZfPW 2022, 178, 181.

[86] *Ders.*, ZfPW 2022, 178, 191.

[87] *Ders.*, ZfPW 2022, 178, 191 f.

[88] BGH, 2.2.1996 – V ZR 239/94, NJW 1996, 1339, 1341; *Kuntz*, ZfPW 2022, 178, 186.

[89] *Kuntz*, ZfPW 2022, 178, 186.

maschinell lernenden Systemen nicht vorhersehbar, wie sich der *Input* in dem generierten *Output* niederschlage.[90] Mit *Input* meint *Kuntz* wohl nicht nur die im konkreten Anwendungsfall eingegebenen Daten, sondern auch die Trainingsdaten.

Die Daten, die im „Inneren" der KI relevant seien, also die Bewertungen und Gewichtungen der Daten und einzelner Parameter, seien kein Wissen im Rechtssinne.[91] Das überzeugt auch vor dem Hintergrund, dass bei Menschen nur explizites Wissen zugerechnet wird: Die Gedanken, Abwägungsgesichtspunkte o. Ä. gelten als implizites Wissen und für die Zwecke der Wissenszurechnung als nicht vorhanden.[92]

Kuntz kommt daher zu dem Ergebnis, dass es erhöhte „Wissensrisiken" beim Einsatz von KI gebe: Setzt ein Mensch KI ein, gibt er bewusst die Kontrolle darüber ab, wie Daten gewonnen und organisiert werden würden. [93] Gespeichert werden muss deshalb zum einen der *Output* des Systems. Sofern die Informationsverwaltung beherrschbar ist, ist zum anderen der zur Verfügung bestehende *Input* zu speichern. Die Informationsverwaltung muss nicht perfekt sein, sondern sich am Stand der Technik orientieren. Die bloße Verfügbarkeit von Daten führt – ebenso wie bei impliziten „Daten" – nicht zu einer Wissenszurechnung.

Für die Arbeitgeberin, die ein maschinell lernendes System einsetzt, folgt daraus, dass sie sich das Wissen über den *Output* und auch teilweise über den *Input* zurechnen lassen muss. Nicht zurechnen lassen muss sie sich aber implizites Wissen, also Wissen, dass sich auf das „Innere" des Systems bezieht.

Auf den oben genannten Beispielsfall [94] bezogen ist der Arbeitgeberin das Wissen über die konkreten Vorgänge im Inneren des Systems nicht zuzurechnen. Das führt dazu, dass sie die „im Verkehr erforderliche Sorgfalt" nicht außer Acht lässt und daher nicht fahrlässig handelt. Sie hat den Verstoß

---

[90] *Ders.*, ZfPW 2022, 178, 187.
[91] *Ders.*, ZfPW 2022, 178, 200.
[92] *Linke*, Digitale Wissensorganisation, 2021, S. 245; a. A.: *Hacker*, RW 2018, 243, 278 ff.
[93] *Kuntz*, ZfPW 2022, 178, 192.
[94] Kapitel 9 B.I.1. (S. 310).

gegen das Benachteiligungsverbot gem. § 15 Abs. 1 S. 1 AGG daher nicht zu vertreten.

b) Zurechnung des Verschuldens der Herstellerin gem. § 278 S. 1 BGB

Wenn ein Vertretenmüssen nicht über die Grundsätze der Wissenszurechnung in Betracht kommt, kann der Arbeitgeberin aber ein solcher „Fehler" wie im geschilderten Beispiel ggf. aufgrund des Verschuldens der Herstellerin gem. § 278 S. 1 BGB zugerechnet werden. Das setzt voraus, dass der Pflichtenkreis der Herstellerin auch umfasst, dass Fehler, die „im Inneren" des Systems liegen, verhindert werden müssen. Außerdem muss die Herstellerin Erfüllungsgehilfin der Arbeitgeberin sein, sodass ihr das Verschulden der Herstellerin nach § 278 S. 1 BGB zugerechnet werden kann.

Der Pflichtenkreis der Herstellerin wird zukünftig maßgeblich durch die Vorgaben des KI-VO-KOM bestimmt. Er richtet sich vor allem an Anbieterinnen, d. h. Personen, die die KI-Systeme in Verkehr bringen oder in Betrieb nehmen.[95] Angenommen, die Herstellerin bringt das KI-System in den Verkehr, ist sie Anbieterin i. S. d. KI-VO-KOM und muss die Pflichten nach dem KI-VO-KOM wahren. Nach dem KI-VO-RAT sind auch Produktherstellerinnen, die KI-Systeme zusammen mit ihrem Produkt unter ihrem Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen, vom Anwendungsbereich der Verordnung erfasst. [96] Im oben genannten Beispielsfall[97] handelt es sich um ein Hochrisiko-KI-System[98], d. h. die Anbieterin muss unter anderem ein Risikomanagementsystem einrichten und die Qualität der Trainingsdaten sicherstellen.[99] Das System muss also den technischen Standards entsprechen und die Risiken, die vom KI-System ausgehen könnten, müssen hinreichend abgeschätzt werden, damit entsprechende (technische) Maßnahmen getroffen werden können. Zwar handelt die Herstellerin oder die Anbieterin nicht automatisch fahrlässig, wenn sich – wie im obigen Beispielsfall – ein nicht durch den Menschen

[95] S. dazu: Kapitel 10 A. (S. 341).
[96] Kapitel 5 A.IV.3.b) (S. 79).
[97] Kapitel 9 B.I.1. (S. 310).
[98] Kapitel 5 A.IV.5. (S. 82).
[99] Kapitel 10 A. (S. 341).

beherrschbares Risiko des Systems realisiert.[100] Zu vertreten hat die Anbieterin den Fehler des maschinell lernenden Systems aber jedenfalls dann, wenn es nicht den technischen Standards entspricht.[101] Im Beispielsfall hätte das System Bewerberinnen asiatischer Herkunft erkannt, wären die technischen Standards eingehalten worden.[102] Die Herstellerin bzw. Anbieter handelte mithin fahrlässig und hat den Fehler des Systems zu vertreten.

Außerdem muss die Herstellerin Erfüllungsgehilfin der Arbeitgeberin sein. Erfüllungsgehilfin ist grundsätzlich, wer nach den „tatsächlichen Gegebenheiten mit dem Willen der Schuldnerin bei der Erfüllung einer diesem obliegende Verbindlichkeit als ihre Hilfsperson tätig wird“[103]. Das erfordert es, die Pflichten der Schuldnerin genau festzulegen. Nach der ständigen Rechtsprechung des BGH ist etwa der Herstellerin einer Kaufsache nicht Erfüllungsgehilfin der Händlerin, die die Sache an ihre Kundinnen verkauft.[104] Die Verkäuferin ist gem. § 433 Abs. 1 BGB verpflichtet, der Käuferin die Sache zu übergeben und das Eigentum an der Sache zu verschaffen. Sie schuldet hingegen nicht die Herstellung der Sache. Im Anbahnungsstadium des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis ist die Arbeitgeberin hingegen gem. § 12 Abs. 1 AGG dazu verpflichtet, die erforderlichen Maßnahmen zum Schutz vor Benachteiligungen wegen eines in § 1 genannten Grunds zu treffen. Setzt sie ein algorithmisches System ein, muss die Arbeitgeberin mithin auch sicherstellen, dass keine diskriminierenden Parameter und Kriterien verwendet werden.[105] Indem sie das System der Herstellerin nutzt, überträgt sie die ihr nach § 12 Abs. 1 AGG obliegende Verpflichtung auf die Herstellerin und setzt sie zur Erfüllung einer

---

[100] *Burchardi*, EuZW 2022, 685, 687; vgl. dazu auch: *Wagner*, AcP 217 (2017), 707, 733 f.

[101] *Burchardi*, EuZW 2022, 685, 687.

[102] Kapitel 9 B.I.1. (S. 310).

[103] BeckOK BGB/*Lorenz*, § 278 BGB Rn. 11; Staudinger (2019)/*Caspers*, § 278 BGB Rn. 18.

[104] BGH, 2.4.2014 – VIII ZR 46/13, NJW 2014, 2183, 2185.

[105] *Höpfner/Daum*, ZfA 2021, 467, 498; vgl. auch: BAG, 22.8.2013 – 8 AZR 563/12, NZA 2014, 82, 85.

ihr obliegenden Verbindlichkeit ein. Etwaiges Verschulden der Herstellerin ist der Arbeitgeberin daher gem. § 278 S. 1 BGB zuzurechnen.[106]

Die Herstellerin hat im Beispielsfall fahrlässig gehandelt und hat den Fehler zu vertreten. Da sie Erfüllungsgehilfin der Arbeitgeberin ist, wird ihr Verschulden der Arbeitgeberin gem. § 278 S. 1 BGB zugerechnet.

2. § 278 S. 1 BGB analog bei algorithmischen Systemen

Kann die Ursache der Benachteiligung durch das System nicht auf ein menschliches Handeln zurückgeführt werden, ist die Frage, ob man § 278 S.1 BGB analog anwenden kann.[107] Das algorithmische System wäre dann Erfüllungsgehilfin der Arbeitgeberin. Die Ursache einer Benachteiligung kann durch das System selbst herbeigerufen werden, wenn es sich um ein maschinell lernendes System handelt. Bei maschinell lernenden Systemen kann das System sein Verhalten aufgrund der gewonnenen Eindrücke selbst anpassen, sodass es zu benachteiligenden Ergebnissen kommen kann, die nicht auf einer menschlichen Einflussnahme basieren.[108]

Für eine analoge Anwendung bedarf es einer planwidrigen Regelungslücke und einer vergleichbaren Interessenlage.[109] Eine Regelungslücke besteht – wie *Höpfner/Daum* zurecht ausführen – nicht: Bei maschinell lernenden Systemen ist bekannt, dass eine mittelbare Benachteiligung womöglich hervorgerufen wird.[110] Die Arbeitgeberin und auch die Herstellerin müssen das System daher auf eine mögliche mittelbare Benachteiligung hin überprüfen und entsprechende Vorkehrungen treffen. Tun sie das nicht, haftet die Arbeitgeberin entweder direkt oder ihr wird das Verschulden der Herstellerin über § 278 S. 1 BGB zugerechnet. Jedenfalls scheitert eine analoge Anwendung des § 278 BGB daran, dass keine vergleichbare Interessenlage vorliegt: Ein algorithmisches System kann nicht die im Verkehr erforderliche

---

[106] *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 412; s. dazu auch: *Höpfner/Daum*, ZfA 2021, 467, 498.

[107] *Lohmann/Preßler*, RDi 2021, 538, 544.

[108] *Zech*, ZfPW 2019, 198, 200 f.

[109] Vgl. *Möllers*, Juristische Methodenlehre, 4. Aufl. 2021, S. 253 ff.

[110] *Höpfner/Daum*, ZfA 2021, 467, 499.

Sorgfalt außer Acht lassen und mithin nicht *schuldhaft* handeln.[111] *Hacker* differenziert zunächst danach, wie hoch der Grad der Autonomie der KI-Agenten (KIA) ist[112]: Jedenfalls bei vollständig autonomen KIA sei die Personenähnlichkeit mit Blick auf § 278 S. 1 BGB zu bejahen. Dieser Ansatz soll aber an der Stelle nicht weiterverfolgt werden, weil es sich bei den untersuchten Systemen nicht um derart autonome KIA handelt, sondern um bloß unterstützende Systeme, die keinen hohen Autonomiegrad aufweisen.

Außerdem wird vorgebracht, dass gem. § 15 Abs. 1 S. 2 AGG das Vertretenmüssen der Arbeitgeberin zunächst vermutet werde. Auf eine Zurechnung komme es nicht mehr an.[113] Das Argument kann aber nicht überzeugen: Die Frage nach einer Beweislastumkehr und einer Zurechnung des Verschuldens über § 278 BGB sind zwei verschiedene Fragen und bedingen sich nicht gegenseitig.[114]

Schließlich argumentiert *Thüsing*, dass es in der Praxis ohnehin nicht auf die Frage nach der Zurechnung ankomme, weil eine ausschließlich automatisierte Entscheidung eines Systems nicht vorliege:[115] Art. 22 DSGVO verbiete eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung. Es komme daher gar nicht dazu, dass ein System eigenständig handele. Dieser Argumentation ist aber ebenfalls entgegenzuhalten, dass die Frage nach der Zurechnung nicht mit der Frage nach einem Verbot automatisierter Entscheidung nach Art. 22 DSGVO gleichgesetzt werden kann.

---

[111] *Benecke*, in: Brose/Greiner/Rolfs u.a. (Hrsg.), Grundlagen des Arbeits- und Sozialrechts, 2021, S. 73, 79; *Borges*, CR 2022, 553, 556; *Freyler*, NZA 2020, 284, 289; *Günther/Böglmüller*, BB 2017, 53, 55; *Keßler*, MMR 2017, 589, 593; *Konertz/Schönhof*, Das technische Phänomen „Künstliche Intelligenz" im allgemeinen Zivilrecht, 2020, S. 117; *Lewinski/Barros Fritz*, NZA 2018, 620, 624; *Zech*, ZfPW 2019, 198, 211.

[112] *Hacker*, RW 2018, 243, 251 ff.

[113] *Freyler*, NZA 2020, 284, 288; *Lewinski/Barros Fritz*, NZA 2018, 620, 623.

[114] Vgl. *Lewinski/Barros Fritz*, NZA 2018, 620, 623; *Wimmer*, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, 2021, S. 414.

[115] MüKoBGB/*Thüsing*, § 3 AGG Rn. 34.

3. Geringer Anwendungsbereich des § 15 Abs. 1 S. 1 AGG

Die praktische Bedeutung des § 15 Abs. 1 AGG ist allerdings eher gering.[116] Damit die Voraussetzungen aus § 15 Abs. 1 S. 1 AGG erfüllt sind, muss die Bewerberin beweisen, dass sie ohne Benachteiligung eingestellt worden wäre. Die Bewerberin müsste also beweisen, dass sie am besten qualifiziert gewesen wäre. Das wird kaum gelingen.[117] Die Beweiserleichterung nach § 22 AGG ist für die haftungsausfüllende Kausalität – mithin den Nachweis, dass die betroffene Person ohne die Benachteiligung eingestellt worden wäre – nicht anwendbar.[118]

II. Entschädigung nach § 15 Abs. 2 S. 1 AGG

Bedeutender ist der Entschädigungsanspruch nach § 15 Abs. 2 S. 1 AGG für immaterielle Schäden.[119] Mit der Benachteiligung wegen eines Merkmals nach § 1 AGG geht regelmäßig eine Persönlichkeitsrechtsverletzung einher, die nach § 15 Abs. 2 S. 1 AGG entschädigungspflichtig ist.[120]

1. Beweiserleichterung nach § 22 AGG bei algorithmischen Systemen

Der Anspruch nach § 15 Abs. 2 S. 1 AGG ist verschuldensunabhängig. Die Bewerberin muss darlegen und beweisen, dass gegen das Benachteiligungsverbot verstoßen wurde. Nach § 22 AGG kommt ihr aber eine Beweislasterleichterung zugute: Diese Norm ordnet an, dass die andere Partei (die Arbeitgeberin) die Beweislast dafür trägt, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligung vorgelegen hat, wenn im Streitfall die eine Partei (die Arbeitnehmerin) Indizien beweist, die eine Benachteiligung wegen eines in § 1 AGG genannten Grunds vermuten lassen. Bei einer möglichen Benachteiligung durch ein algorithmisches System muss die Arbeitnehmerin also Indizien vorbringen, dass das System eine benachteiligende Auswahlentscheidung getroffen hat. Problematisch sind dabei zwei Punkte. Zum einen ist ein maschinell lernendes System nicht

---

[116] *Benecke*, in: Brose/Greiner/Rolfs u.a. (Hrsg.), Grundlagen des Arbeits- und Sozialrechts, 2021, S. 73, 74.

[117] *Dzida/Groh*, NJW 2018, 1917, 1921.

[118] BeckOK Arbeitsrecht/*Roloff*, § 22 AGG Rn. 1.

[119] *Freyler*, NZA 2020, 284, 290.

[120] ErfK/*Schlachter*, § 15 AGG Rn. 8.

transparent, sodass eine Benachteiligung durch das System nicht offensichtlich ist. [121] Zum anderen sind die im System enthaltenen Algorithmen häufig Betriebs- oder Geschäftsgeheimnis des jeweiligen Unternehmens.[122]

Wurden etwa aufgrund unvollständiger Trainingsdaten Männer gegenüber Frauen bevorzugt und daher überwiegend zum Vorstellungsgespräch eingeladen, kann die Bewerberin in den allermeisten Fällen keine hinreichenden Indizien darlegen, warum das eingesetzte System voreingenommen war.[123] Sie hat keinen Einblick in das System, unabhängig davon, ob die Benachteiligung durch einen Fehler bei der Programmiererin zustande gekommen oder auf das System selbst zurückzuführen ist. Müssen beim Einsatz maschinell lernender Systeme daher andere Maßstäbe für § 22 AGG gelten?

a) Blackbox-Auswertungen als Indiz

Martini schlägt vor, § 22 AGG dahingehend zu ergänzen, dass *Blackbox*-Auswertungen für algorithmenbasierte Verfahren als Indiz ausreichen, sollten dem Einzelnen nur die Möglichkeit eines Blackbox-Testes zur Verfügung stehen.[124] Ein solcher – auch funktionaler Test genannt – betrachtet das von außen sichtbare Verhalten der Software.[125] Nur die *Inputs* und die *Outputs*, d. h. Eingaben und Ergebnisse der Software, werden betrachtet.[126] Gegenüber einem sog. Whitebox-Test, der die innere Struktur der Software betrachtet und somit besagt, wie das maschinell lernende System arbeitet und aufgebaut

---

[121] *Burchardi*, EuZW 2022, 685, 656 f.; *Freyler*, NZA 2020, 284, 290; *Kullmann*, in: Beyer/Erler/Hartmann u.a. (Hrsg.), Privatrecht 2050 - Blick in die digitale Zukunft, 2020, S. 227, 243;

[122] *Kullmann*, in: Beyer/Erler/Hartmann u.a. (Hrsg.), Privatrecht 2050 - Blick in die digitale Zukunft, 2020, S. 227, 243; *Freyler*, NZA 2020, 284, 290; s. dazu auch Kapitel 4 A.I.2. (S. 41).

[123] *Lauscher/Legner*, ZfDR 2022, 367, 378; vgl. *Martini*, Blackbox Algorithmus, 2018, S. 247; *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 59.

[124] *Martini*, Blackbox Algorithmus, 2018, S. 247 f.; *ders.*, JZ 2017, 1017, 1024.

[125] Auer-Reinsdorff/Conrad/*Schmidt*, § 1 V. 4. a) Rn. 350.

[126] *Kroll/Huey/Barocas u.a.*, Univ. Pa. Law Rev. 165 (2017), 633, 650.

ist[127], ist der *Blackbox*-Test der weniger aussagekräftige Test.[128] Als Bewerberin oder Arbeitgeberin steht einem der Whitebox-Test aber normalerweise nicht als Möglichkeit zur Verfügung, weil man weder den Zugang zum Quellcode noch zur Modellierung des Systems hat.[129] Eine Beschäftigte, die einen Anspruch auf Entschädigung nach § 15 Abs. 2 S. 1 AGG geltend macht, muss somit als Indiz Auswertungen eines *Blackbox*-Testes vorweisen. Die Arbeitgeberin kann den Vorwurf einer Benachteiligung dadurch entkräften, indem sie etwa vorlegt, welche technisch-organisatorischen Maßnahmen sie einsetzt, um Benachteiligungen durch algorithmische Systeme zu verhindern.[130]

Je nach Komplexität des Systems ist aber auch ein Blackbox-Test nur geringfügig aussagekräftig.[131] Um Aussagen darüber zu treffen, ob ein System zu benachteiligenden Ergebnissen führt, reicht es nicht aus, wenn man nur die *Input-* und *Output-Daten* hat. Vielmehr muss man auch die Parameter, Gewichtungen und tatsächlichen Umstände der Entscheidung kennen.[132] Eine „sichere" Lösung ist ein Blackbox-Test somit nicht, um Benachteiligungen aufzudecken.

b) Indizien aufgrund der Informationspflichten nach Art. 12 ff. DSGVO

Nach Art. 13 f. DSGVO muss die Verantwortliche bestimmte Informationspflichten erfüllen.[133] Die Informationen könnten als Indizien im Rahmen von § 22 AGG vorgebracht werden. Schließlich müssen bei einer automatisierten Entscheidungsfindung nach Art. 13 Abs. 2 lit. f DSGVO aussagekräftige Informationen über die involvierte Logik bereitgestellt werden. Wie bereits herausgearbeitet worden ist, sollte die Informationspflicht auch bei nicht ausschließlich automatisierter Entscheidungsfindung gelten.[134] Allerdings ist Art. 13 Abs. 2 lit. f DSGVO in

---

[127] Auer-Reinsdorff/Conrad/*Schmidt*, § 1 V. 4. b) Rn. 353.
[128] *Kroll/Huey/Barocas u.a.*, Univ. Pa. Law Rev. 165 (2017), 633, 650 f.
[129] *Martini*, Blackbox Algorithmus, 2018, S. 45.
[130] *Ebd.*, S. 238.
[131] *Ebd.*, S. 45 f.
[132] *Ebd.*, S. 45.
[133] S. dazu bereits unter: Kapitel 7 B. (S. 246).
[134] Kapitel 7 B.III. (S. 250).

seinem Anwendungsbereich beschränkt und gewährleistet keine umfassende Information über das System: Wie der BGH in seinem Urteil ausgeführt hat, werde ein transparentes Verfahren für die betroffene Person vielmehr dadurch erreicht, „dass für den Betroffenen ersichtlich ist, welche konkreten Umstände als Berechnungsgrundlage in der Ermittlung des Wahrscheinlichkeitswerts eingeflossen sind“[135]. Die abstrakten Vergleichsgruppen und Gewichtungen müssen nicht offengelegt werden, vielmehr reicht es aus, wenn die eingeflossenen Daten und der „Umstand ihres Einflusses“ auf das konkrete Berechnungsergebnis zu offenbaren sind.[136]

Damit die betroffene Person Indizien für eine Benachteiligung sammeln kann, braucht sie aber gerade den Vergleich zu anderen Gruppen. [137] Die Informationspflichten aus Art. 13 f. DSGVO sind somit nicht hilfreich, wenn es darum geht, Indizien für eine Benachteiligung zu sammeln.[138]

c) Zwei-Stufen-Modell der Darlegungslast nach Grünberger

Eine überzeugende Möglichkeit, mithilfe derer das Kausalitätsproblem angemessen gelöst werden kann, ist hingegen das von *Grünberger* vorgeschlagene „Zwei-Stufen-Modell der Darlegungslast“[139], was im Prinzip auf das Institut der sekundären Darlegungslast aufbaut und streng genommen ein Vier-Stufen-Modell ist.

Auf die sekundäre Darlegungslast hat der BGH beim VW-Abgasskandal zurückgegriffen.[140] Grundsätzlich hätte die Klägerin darlegen und beweisen müssen, dass der Vorstand von VW oder eine andere verfassungsmäßige Vertreterin im Sinne des § 31 BGB die objektiven und subjektiven Tatbestandsvoraussetzungen des § 826 BGB verwirklicht hat.[141] Die Klägerin hatte jedoch keine Einblicke in die internen Unternehmensabläufe, sodass es für die Klägerin kaum möglich war, darzulegen und beweisen, was der

---

[135] BGH, 28.1.2014 – VI ZR 156/13, NJW 2014, 1235, 1237 Rn. 29.
[136] BGH, 28.1.2014 – VI ZR 156/13, NJW 2014, 1235, 1237 Rn. 29.
[137] S. Kapitel 7 B.V.3. (S. 259).
[138] *Martini*, Blackbox Algorithmus, 2018, S. 247; *Grünberger*, ZRP 2021, 232, 233 f.
[139] *Grünberger*, ZRP 2021, 232, 235 f.
[140] BGH, 11.5.2021 – VI ZR 154/20, NJOZ 2021, 1049.
[141] BGH, 11.5.2021 – VI ZR 154/20, NJOZ 2021, 1049, 1050 Rn. 14.

Vorstand wusste.[142] In solchen Fällen wird der Grundsatz, dass die Partei, die den Anspruch geltend macht, die volle Darlegungs- und Beweislast trägt, eingeschränkt: Wenn die Partei keine nähere Kenntnis von den maßgeblichen Umständen hat und es ihr nicht möglich ist, den Sachverhalt weiter aufzuklären, trifft die Gegnerin eine sekundäre Darlegungslast, in deren Rahmen sie weitere Nachforschungen anstellen muss.[143] Kommt sie ihrer sekundären Darlegungslast nicht nach, gelten die Behauptungen der Anspruchstellerin gem. § 138 Abs. 3 ZPO als zugestanden.[144]

Wenn maschinell lernende Systeme eingesetzt werden, liegt ein entscheidender Unterschied zum Fall des VW-Abgasskandals darin, dass die Arbeitgeberin in aller Regel auch nicht vollständig nachvollziehen kann, wie das System funktioniert.[145] Die Bewerberin hat aber erst recht keinen Einblick in die Abläufe des Systems und kann nicht darlegen und beweisen, ob sie gerade *wegen* eines Merkmals nach § 1 AGG benachteiligt wurde.

Grünberger schlägt vor, dass die Bewerberin ihrer (primären) Darlegungslast genüge, wenn sie darlege, dass ein algorithmisches System bei der Entscheidungsfindung eingesetzt worden sei.[146] Das ist in der Regel keine Hürde für sie, weil sie entweder in die Verarbeitung eingewilligt hat gem. Art. 6 Abs. 1 S. 1. lit. a DSGVO, § 26 Abs. 2 BDSG oder sonst über die Rechtsgrundlage nach der DSGVO oder dem BDSG und damit das Verarbeitungserfordernis durch das algorithmische System in Kenntnis gesetzt wurde.[147] Andere Stimmen in der Literatur erachten es als unzureichend, wenn die Bewerberin als Indiz darlegt, dass ein algorithmisches System eingesetzt wurde.[148] Die von einer Benachteiligung betroffene Person müsse vielmehr Indizien vorbringen, die den Verstoß gegen ein

---

[142] BGH, 11.5.2021 – VI ZR 154/20, NJOZ 2021, 1049, 1050 Rn. 16.
[143] BGH, 11.5.2021 – VI ZR 154/20, NJOZ 2021, 1049, 1050 Rn. 14.
[144] BGH, 11.5.2021 – VI ZR 154/20, NJOZ 2021, 1049, 1050 Rn. 14.
[145] *Grünberger*, ZRP 2021, 232, 234.
[146] *Ders.*, ZRP 2021, 232, 234.
[147] *Ders.*, ZRP 2021, 232, 234.
[148] BeckOGK/*Benecke*, § 22 AGG Rn. 46; *Freyler*, NZA 2020, 284, 290; *Höpfner/Daum*, ZfA 2021, 467, 495.

Benachteiligungsverbot als überwiegend wahrscheinlich vermuten lassen.[149] Indizien für eine Benachteiligung könnten sich etwa aus den Trainingsdaten oder den verwendeten Parametern ergeben.[150] Allerdings ergibt sich eine Benachteiligung häufig nicht direkt aus den Trainingsdaten oder verwendeten Parametern, vielmehr benötigt die betroffene Person auch Informationen über die Vergleichsgruppen. Diese Information werden ihr aber nicht über die Informationspflichten nach Art. 12 ff. DSGVO zuteil.[151]

Grünberger ist daher zuzustimmen, dass auf der ersten Stufe zunächst die Bewerberin darlegen muss, dass ein maschinell lernendes System verwendet wurde. Auf der zweiten Stufe muss die Arbeitgeberin ihre Darlegungslast erfüllen. Dadurch, dass auch die Arbeitgeberin keinen vollständigen Einblick in das verwendete System hat, müssen die Anforderungen an die sekundäre Darlegungslast anders ausgestaltet werden. Die Arbeitgeberin erfülle, so *Grünberger*, die Anforderungen an die sekundäre Darlegungslast, wenn sie substanziiert darlege, dass das eingesetzte System den nach Wissenschaft und Technik möglichen „Fairnessanforderungen" genüge.[152] Unabhängige Zertifizierungseinrichtungen könnten entsprechende Regelwerke aufstellen, deren Einhaltung der Arbeitgeberin entsprechende Sicherheit biete.[153] Wichtig sei dabei, dass die Einrichtungen die Regelwerke mithilfe der relevanten *Stakeholder* entwickeln würden. Damit diese Regelwerke den Fairnessanforderungen der maschinell lernenden Systeme genügen könnten, sei es unerlässlich, die relevanten Akteure mit einzubeziehen.[154] Diese Ausführungen überzeugen. Allerdings müssen die *Fairnessanforderungen* näher konkretisiert werden. Angebracht wäre es etwa, eine Testpflicht für derartige Systeme rechtlich zu verankern.[155] Der Prozess der Entwicklung und Testung des algorithmischen Systems muss dokumentiert werden.[156] Bei

---

[149] BAG, 21.6.2012 – 8 AZR 364/11, NZA 2012, 1345, 1348; ErfK/*Schlachter*, § 22 AGG Rn. 3; *Martini*, JZ 2017, 1017, 1024; *Höpfner/Daum*, ZfA 2021, 467, 495.

[150] *Höpfner/Daum*, ZfA 2021, 467, 495.

[151] S. dazu bereits: Kapitel 9 B.II.1.b) (S. 320).

[152] *Grünberger*, ZRP 2021, 232, 234 f.; s. zu Fairnessanforderungen auch: *Hütt/Schubert*, in: Mainzer (Hrsg.), Philosophisches Handbuch Künstliche Intelligenz, 2020, 10 f.

[153] *Grünberger*, ZRP 2021, 232, 235.

[154] S. dazu etwa auch: *Bryson/Haataja*, Competition Policy International 14.03.2022, 5.

[155] *Sesing/Tschech*, MMR 2022, 24, 26 f.

[156] *Dies.*, MMR 2022, 24, 28, vgl. *Glatzner*, DuD 2020, 312, 315.

Hochrisiko-KI-Systemen kann man es auch als ausreichend für die sekundäre Darlegungslast der Arbeitgeberin ansehen, wenn sie darlegt, dass sie entsprechend den Vorschriften des KI-VO-KOM ihr System entwickelt hat.[157] Nach Art. 11 Abs. 1 KI-VO-KOM muss etwa eine technische Dokumentation erstellt werden, aus der hervorgeht, dass das bestimmte Hochrisiko-KI-System den Anforderungen genügt, die allgemein für Hochrisiko-KI-Systeme gelten. Liegt eine solche Dokumentation nicht vor, kann die betroffene Person das Nichtvorliegen der Dokumentation auch als Indiz für eine Benachteiligung verwenden.

Kann die Bewerberin die Vermutung, dass keine Benachteiligung vorliegt, widerlegen, muss die Arbeitgeberin das konkrete Entscheidungsmodell erklären und/oder die Gründe für die Entscheidung offenlegen.[158] Kann sie dem nicht nachkommen, kommt sie ihrer Darlegungslast nicht nach. Der Einwand der Beschäftigten, dass eine Benachteiligung vorliege, gilt gem. § 138 Abs. 3 ZPO als zugestanden.[159]

2. Fazit: gerechte Lösung durch Zwei-Stufen-Modell der Darlegungslast

§ 22 AGG ist für Personen, die eine Benachteiligung wegen eines maschinell lernenden Systems geltend machen wollen, unzureichend. Die Bewerberin wird in aller Regel keine Indizien vorbringen können, die eine Benachteiligung wegen eines in § 1 AGG genannten Grunds vermuten lassen. Anders als bei einer Stellenausschreibung, bei der etwa eine bestimmte Wortwahl ein Indiz für eine Benachteiligung sein kann, sind maschinell lernende Systeme nicht hinreichend transparent.[160]

Damit § 22 AGG im Kontext maschinell lernender Systeme seinen Normzweck erfüllt, muss das Zwei-Stufen-Modell der Darlegungslast nach *Grünberger* greifen.[161] Die Bewerberin genügt auf der ersten Stufe ihrer Darlegungslast, wenn sie darlegt, dass ein maschinell lernendes System

---

[157] S. *Grünberger*, ZRP 2021, 232, 235.

[158] *Ders.*, ZRP 2021, 232, 235.

[159] I. E. wohl auch *ders.*, ZRP 2021, 232, 235.

[160] Kapitel 4 A. (S. 40).

[161] Im Ergebnis so auch: *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 71.

eingesetzt wurde. Auf der zweiten Stufe muss die Arbeitgeberin darlegen, dass das System den technischen Fairnessanforderungen genügt, d. h. etwa, ob die Anforderungen an das Hochrisiko-KI-System nach dem KI-VO-KOM gewahrt wurden.[162] Widerlegt die Bewerberin die Vermutung, dass eine Benachteiligung vorliegt, muss die Arbeitgeberin das System und die Entscheidung offenlegen. Das Modell schafft einen angemessenen Ausgleich zwischen den Interessen der Bewerberin und der Arbeitgeberin, da mit jeder Stufe die Anforderungen an die Darlegungslast für beide Seiten erhöht werden.

C. Zwischenergebnis zum Schutzrahmen des AGG

1. Wird ein algorithmisches System im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis eingesetzt, ist der Anwendungsbereich des AGG in sachlicher und in persönlicher Hinsicht eröffnet.[163] Dass bereits Bewerberinnen in den Anwendungsbereich des AGG fallen, ergibt sich aus § 6 Abs. 1 S. 2 AGG. Werden im Bewerbungsverfahren Trainingsdaten gesammelt, dient dieser Schritt dazu, ein System zu entwickeln, das bei der Auswahl künftiger Bewerberinnen eingesetzt werden kann. In solchen Fällen ist der Anwendungsbereich des AGG bereits bei der beschriebenen Sammlung von Trainingsdaten eröffnet.[164] Das maschinell lernende System legt schon in diesem Zeitpunkt die Bedingungen fest, die für den Zugang zu unselbständiger und selbständiger Erwerbstätigkeit relevant sind (§ 2 Abs. 1 Nr. 1 AGG).

2. Bereits gegen eine potenzielle Benachteiligung wegen unzureichender Trainingsdaten vorzugehen, ist in Deutschland bislang nicht möglich, weil es auf nationaler Ebene keine Verbandsklage zur Durchsetzung des AGG in Fällen potenzieller Benachteiligungen gibt. Bei einem Fall, den der EuGH im Hinblick auf potenzielle Benachteiligungen zu entscheiden hatte,[165] lag die Besonderheit darin, dass eine Vereinigung

---

[162] S. dazu noch unter: Kapitel 10 (S. 341).
[163] Kapitel 9 A.I. (S. 293).
[164] Kapitel 9 A.I.2. (S. 294).
[165] Kapitel 9 A.I.2. (S. 294).

von Rechtsanwälten nach dem anwendbaren italienischen Recht befugt war, gegen die Benachteiligung einer Personengruppe zu klagen, obwohl es keine Geschädigte gab.[166]

3. Algorithmische Systeme können aus verschiedenen Gründen eine unmittelbare (§ 3 Abs. 1 AGG) oder mittelbare Benachteiligung (§ 3 Abs. 2 AGG) hervorrufen.[167]

4. Eine unmittelbare Benachteiligung liegt vor, wenn eine Person wegen eines in § 1 AGG genannten Grundes eine weniger günstige Behandlung erfährt, als eine andere Person in einer vergleichbaren Situation erfährt, erfahren hat oder erfahren würde (§ 3 Abs. 1 AGG). Anknüpfungspunkt der Benachteiligung ist dabei nicht die Behandlung durch das algorithmischen Systems selbst, sondern die menschliche Letztentscheidung, die wegen Art. 22 DSGVO erforderlich ist.[168] Es kommt also nicht darauf an, ob bereits die Entscheidung durch das algorithmische System eine Behandlung i. S. d. § 3 Abs. 1 AGG ist.

5. Bei einem nicht-lernenden System ist eine unmittelbare Benachteiligung denkbar, wenn z. B. bewusst bestimmte Gruppen beim Einprogrammieren der Entscheidungskriterien nicht berücksichtigt werden. Ursache dafür können z. B. Vorurteile der Entwicklerinnen sein, die im nicht-lernenden System abgebildet werden.[169]

6. Bei maschinell lernenden Systemen wird es eher zu mittelbaren Benachteiligungen kommen. Eine mittelbare Benachteiligung liegt gem. § 3 Abs. 2 AGG vor, wenn dem Anschein nach neutrale Vorschriften, Kriterien oder Verfahren Personen wegen eines in § 1 AGG genannten Grundes gegenüber anderen Personen in besonderer Weise benachteiligen. Die verwendeten Kriterien und Parameter des maschinell lernenden Systems werden – anders als bei nicht-lernenden Systemen – nicht händisch von den Entwicklerinnen einprogrammiert,

---

[166] S. dazu: Kapitel 9 A.I.2. (S. 294); Kapitel 9 A.II.1.a) (S. 296).
[167] S. Kapitel 8 B. (S. 288).
[168] Kapitel 9 A.II.1.a) (S. 296).
[169] Kapitel 8 B.III. (S. 290).

sondern ergeben sich aus der Auswertung der Trainingsdaten. Deshalb sind sie an sich neutral. Wegen unzutreffender Korrelationen können sich dennoch mittelbare Benachteiligungen ergeben.[170] Außerdem kann es sein, dass die Trainingsdatenqualität mangelhaft ist. Wenn in den Trainingsdaten bestimmte Aspekte unzureichend berücksichtigt wurden, kann das ebenfalls zu Benachteiligungen führen.[171] Werden z. B. Frauen häufiger mit einem Teilzeitjob in Verbindung gebracht, kann es sein, dass ein maschinell lernendes System Frauen grundsätzlich nicht als geeignete Personen für einen Vollzeitjob vorschlägt.

7. Der Vorschlag von *Spiecker gen. Döhmann* und *Towfigh*, den Anwendungsbereich des § 1 AGG auch auf eine Benachteiligung zu erstrecken, die sich „aus einer Beziehung ergibt, die nur auf statistischer Korrelation beruht", überzeugt aus drei Gründen nicht.[172] Erstens fehlt einem solchen Benachteiligungsmerkmal der materielle Charakter der sonstigen in § 1 AGG genannten Merkmale, weil sich der Vorschlag nicht auf den Entscheidungsgrund, sondern das Entscheidungsverfahren bezieht. Zweitens steht der Vorschlag in Konflikt mit § 7 Abs. 1 Hs. 2 AGG, weil man eine Diskriminierung, die auf einer Beziehung aufgrund statistischer Korrelation beruht, gem. § 7 Abs. 1 Hs. 2 AGG nicht „nur" annehmen kann. Drittens wird es kaum möglich sein, die Diskriminierung aufgrund statistischer Korrelation nachzuweisen.

8. Gem. § 7 AGG muss die Benachteiligung *wegen* eines in § 1 AGG genannten Merkmals erfolgen (Kausalität).[173] Dabei reicht es aus, wenn die Benachteiligung wegen mehrerer Merkmale (sog. Motivbündel) erfolgt. Da maschinell lernende Systeme mit vielen Daten trainiert werden, wird die Benachteiligung eher nicht nur auf einem Merkmal beruhen. [174] Es kann zudem technisch schwierig sein, einzelne Benachteiligungsparameter zu isolieren. Die Kausalität entfällt nicht

---

[170] Kapitel 8 B.II. (S. 289).
[171] Kapitel 8 B.I. (S. 288).
[172] Kapitel 9 A.II.1.b) (S. 298).
[173] Kapitel 9 A.II.1.c) (S. 298).
[174] Kapitel 9 A.II.2. (S. 301).

deshalb, weil die Entscheidungsträgerin keine Kenntnis der diskriminierenden Parameter hat. Sie macht sich das Ergebnis des Systems zu eigen, indem sie es in ihre Entscheidung mit einbezieht. Somit übernimmt die Entscheidungsträgerin das Haftungsrisiko für Benachteiligungen, wenn sie der vom algorithmischen System vorgeschlagene Entscheidung folgt.

9. Eine unmittelbare Benachteiligung kann im Einzelfall nach §§ 8-10 AGG gerechtfertigt sein. Wenn der Einsatz eines algorithmischen Systems eine positive Maßnahme i. S. d. § 5 AGG ist, kommt auch eine Rechtfertigung nach § 5 AGG in Betracht. Eine solche positive Maßnahme liegt vor, wenn das algorithmische System z. B. konkret für den Anwendungsfall trainiert worden ist, Ziele wie etwa das Geschlechtergleichgewicht in einem Unternehmen zu verbessern.

10. Eine mittelbare Benachteiligung ist gem. § 3 Abs. 1 Hs. 2 AGG gerechtfertigt, wenn die Vorschriften, Kriterien oder Verfahren, die zu einer mittelbaren Benachteiligung führen, durch ein rechtmäßiges Ziel sachlich gerechtfertigt und die Mittel zur Erreichung des Ziels angemessen und erforderlich sind. Die Arbeitgeberin verfolgt in aller Regel ein legitimes Ziel mit dem Einsatz des algorithmischen Systems.[175] Ein solches Ziel liegt etwa darin, die geeignete Kandidatin für eine zu besetzende Stelle zu finden. Das algorithmische System ist grundsätzlich geeignet, das legitime Ziel zu erreichen, wenn es entsprechende Test- und Validierungsverfahren durchlaufen hat und die Arbeitgeberin zudem nachweisen kann, dass die Qualität der Trainingsdaten nach Art. 10 Abs. 5 KI-VO-KOM[176] sichergestellt ist.[177] Die Arbeitgeberin trägt im Streitfall insoweit die Darlegungs- und Beweislast.

11. Auf der Ebene der Erforderlichkeit ist zu prüfen, ob es ein gleich geeignetes, milderes Mittel gegenüber dem Einsatz eines algorithmischen Systems gibt.[178] Herkömmliche Verfahren zur Auswahl

---

[175] Kapitel 9 A.III.2.a) (S. 304).
[176] Kapitel 10 B.I. (S. 345).
[177] Kapitel 9 A.III.2.b)aa) (S. 304).
[178] Kapitel 9 A.III.2.b)bb) (S. 306).

von Personen sind – wie auch bereits im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO deutlich wird – nicht unbedingt milder gegenüber der Auswahl durch algorithmische Systeme. Das liegt daran, dass man je nach Vorgang des Auswahlprozesses bei algorithmischen Systemen die Möglichkeit hat, Probeläufe zu absolvieren. [179] Bei einem herkömmlichen Bewerbungsverfahren hat man i. d. R. nur eine Chance, einen guten (ersten) Eindruck zu hinterlassen.

12. Vorausgesetzt, es gibt kein gleich geeignetes, milderes Mittel, muss der Einsatz des algorithmischen Systems auch angemessen sein. [180] Das bedeutet, dass das System die legitimen Interessen der Personen nicht übermäßig beeinträchtigen darf, die wegen eines in § 1 AGG genannten Grundes mittelbar benachteiligt werden. Das Persönlichkeitsrecht der betroffenen Person würde weniger stark beeinträchtigt werden, wenn die mittelbare Benachteiligung nicht auftritt. Die Gründe einer mittelbaren Benachteiligung sind häufig auf ein unzureichendes Trainingsdatenset zurückzuführen. Im Rahmen der Angemessenheitsprüfung ist erstens zu berücksichtigen, dass es der Arbeitgeberin grundsätzlich zumutbar ist, die Kosten für ein qualitativ höherwertigeres und somit zu weniger Benachteiligungen führendes Trainingsdatenset aufzuwenden. [181] Wenn keine besseren Trainingsdaten verfügbar sind oder es mit unverhältnismäßigen Kosten verbunden wären, bessere Trainingsdaten zu beschaffen, ist das System zweitens nur angemessen, wenn die Arbeitgeberin nachweist, dass das eingesetzte System signifikant und nachweislich zu weniger voreingenommen Ergebnissen kommt als andere (nicht algorithmische) Verfahren.

13. Die Arbeitgeberin haftet bei Verstößen gegen das Benachteiligungsverbot nach § 15 Abs. 1 S. 1 AGG oder § 15 Abs. 2 S. 1 AGG. § 15 Abs. 1 AGG setzt ein Vertretenmüssen der Arbeitgeberin voraus (§ 15 Abs. 1 S. 2 AGG), für dessen Fehlen die Arbeitgeberin

---

[179] S. dazu bereits Kapitel 6 C.IV.2.c)aa) (S. 178).
[180] Kapitel 9 A.III.2.b)cc) (S. 307).
[181] S. Kapitel 9 A.III.2.b)cc) (S. 307).

darlegungs- und beweispflichtig ist.[182] Das Vertretenmüssen richtet sich nach §§ 276 ff. BGB. Beim Umfang des Vertretenmüssens ist zu berücksichtigen, welches Wissen die Arbeitgeberin über das algorithmische System hat. [183] Grundsätzlich muss sich die Arbeitgeberin nach den Grundsätzen der Wissenszurechnung das Wissen über den *Output* (Ergebnis des Systems) und teilweise auch über den *Input* (insbesondere die Trainingsdaten) zurechnen lassen. Ergibt sich aufgrund dieses Wissens, dass die Arbeitgeberin durch den Einsatz des Systems die im Verkehr erforderliche Sorgfalt außer Acht lässt, handelt sie fahrlässig und hat den Verstoß gegen das Benachteiligungsverbot nach § 15 Abs. 1 S. 1 AGG zu vertreten. [184] Nicht zuzurechnen ist der Arbeitgeberin aber das implizite Wissen, also die Vorgänge im „Inneren" des maschinell lernenden Systems. Das sind regelmäßig die vom maschinell lernenden System im Zuge des Trainings vorgenommenen Gewichtungen einzelner Parameter.

14. Handelt die Herstellerin fahrlässig, wird das Verschulden der Herstellerin der Arbeitgeberin gem. § 278 S. 1 BGB zugerechnet.[185] Die Arbeitgeberin hat gem. § 12 Abs. 1 AGG die Pflicht, Maßnahmen zum Schutz vor Benachteiligungen zu treffen. Das umfasst im Kontext algorithmischer Systeme auch, dass sie sicherstellen muss, dass keine diskriminierenden Parameter verwendet werden. Indem sie die Pflicht auf die Herstellerin des Systems überträgt, die die technischen Prüfverfahren durchführt und sicherstellt, dass das System keine Benachteiligungen hervorruft, setzt sie die Herstellerin als Erfüllungsgehilfin ein.

15. § 278 S. 1 BGB ist nicht analog auf algorithmische Systeme selbst anzuwenden, wenn die Ursache der Benachteiligung durch das System nicht auf menschliches Handeln der Herstellerin zurückgeführt werden kann. [186] Das algorithmische System wäre Erfüllungsgehilfin der

---

[182] Kapitel 9 B.I.1. (S. 310).
[183] S. Kapitel 9 B.I.1.a) (S. 311).
[184] Kapitel 9 B.I.1.a) (S. 311).
[185] Kapitel 9 B.I.1.b) (S. 314).
[186] Kapitel 9 B.I.2. (S. 316).

Arbeitgeberin. Eine analoge Anwendung ist richtigerweise abzulehnen: Eine Regelungslücke besteht schon deshalb nicht, weil Arbeitgeberin und die Herstellerin das System auf eine mögliche mittelbare Benachteiligung hin überprüfen und entsprechende Vorkehrungen treffen müssen. Tun sie das nicht, haftet die Arbeitgeberin entweder direkt oder ihr wird – wie soeben ausgeführt – das Verschulden der Herstellerin über § 278 S. 1 BGB zugerechnet. Außerdem kann ein algorithmisches System nicht die im Verkehr erforderliche Sorgfalt außer Acht lassen und daher nicht schuldhaft handeln. Es ist keine am Verkehr teilnehmende Person und kann in Bezug auf § 278 S. 1 BGB auch nicht sinnvoll wie eine solche behandelt werden. Es fehlt daher auch an einer vergleichbaren Interessenlage.

16. Der Anspruch nach § 15 Abs. 1 S. 1 AGG scheitert in der Praxis fast immer, weil die Bewerberin darlegen und beweisen müsste, dass sie die am besten geeignete Kandidatin für die Position gewesen wäre. Dieser Nachweis wird ihr kaum gelingen.[187]

17. Relevanter ist daher der Anspruch auf angemessene Entschädigung nach § 15 Abs. 2 S. 1 AGG. [188] Dieser Anspruch ist verschuldensunabhängig. Die Anspruchstellerin muss im Schadensersatzprozess als nach den allgemeinen Grundsätzen darlegungs- und beweisbelastete Partei Indizien vortragen, die auf eine Benachteiligung i. S. d. AGG schließen lassen. Zwar statuiert § 22 AGG eine Beweiserleichterung: Beweist die eine Partei Indizien, die eine Benachteiligung wegen eines in § 1 AGG genannten Grundes vermuten lassen, trägt die andere Partei die Beweislast dafür, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligung vorgelegen hat. Diese wird bei algorithmischen Systemen aber kaum weiterhelfen, weil die Anspruchstellerin zumeist keinen näheren Einblick in das System hat. Damit § 22 AGG im Kontext algorithmischer Systeme seinen Normzweck erfüllt, muss das von *Grünberger* entwickelte Zwei-Stufen-Modell der Darlegungslast greifen.[189] Bei diesem Modell handelt

[187] Kapitel 9 B.I.3. (S. 318).
[188] Kapitel 9 B.II. (S. 318).
[189] Kapitel 9 B.II.1.c) (S. 321).

es sich eigentlich um ein Vier-Stufen-Modell. Die Bewerberin genügt auf der ersten Stufe ihrer Darlegungslast, wenn sie darlegt, dass ein algorithmisches System eingesetzt wurde. Auf der zweiten Stufe muss die Arbeitgeberin darlegen, dass das System den technischen Fairnessanforderungen genügt, etwa, ob die Anforderungen an das Hochrisiko-KI-System nach dem KI-VO-KOM gewahrt wurden. Widerlegt die Bewerberin auf der dritten Stufe die Vermutung, dass keine Benachteiligung vorliegt, muss die Arbeitgeberin auf der vierten Stufe das System und die Entscheidung offenlegen. Dieses Modell schafft einen angemessenen Ausgleich zwischen den Interessen der Beschäftigten und der Arbeitgeberin, da mit jeder Stufe die Anforderungen an die Darlegungslast für beide Seiten erhöht werden.

Teil 3

Zusammenfassung

1. Die Untersuchung zeigt, dass Benachteiligungen durch algorithmische Systeme bereits ein alltägliches Phänomen sind und erhebliche Auswirkungen auf einzelne Individuen haben können. Als Beispiel für Gefahren im arbeitsrechtlichen Kontext dient das österreichische Modell *AMAS*, das Arbeitsmarktchancen von Arbeitslosen berechnet.[1]

2. Wird ein algorithmisches System im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis eingesetzt, ist der Anwendungsbereich des AGG in sachlicher und in persönlicher Hinsicht eröffnet.[2] Soll ein algorithmisches System für Auswahl künftiger Bewerberinnen eingesetzt werden, ist der Anwendungsbereich des AGG bereits bei der Sammlung von Trainingsdaten eröffnet.[3] Bereits zu diesem Zeitpunkt gegen eine potenzielle Benachteiligung wegen unzureichender Trainingsdaten vorzugehen, ist in Deutschland bislang nicht möglich, weil es auf nationaler Ebene keine Verbandsklage zur Durchsetzung des AGG in Fällen potenzieller Benachteiligungen gibt.[4]

3. Algorithmische Systeme können aus verschiedenen Gründen eine unmittelbare (§ 3 Abs. 1 AGG) oder mittelbare Benachteiligung (§ 3 Abs. 2 AGG) hervorrufen.[5]

4. Eine unmittelbare Benachteiligung liegt vor, wenn eine Person wegen eines in § 1 AGG genannten Grundes eine weniger günstige Behandlung

---

[1] Kapitel 8 A.III. (S. 284).
[2] Kapitel 9 A.I. (S. 293).
[3] Kapitel 9 A.I.2. (S. 294).
[4] S. dazu: Kapitel 9 A.I.2. (S. 294); Kapitel 9 A.II.1.a) (S. 296).
[5] S. Kapitel 8 B. (S. 288).

erfährt, als eine andere Person in einer vergleichbaren Situation erfährt, erfahren hat oder erfahren würde (§ 3 Abs. 1 AGG). Anknüpfungspunkt der Benachteiligung ist dabei nicht die Behandlung durch das algorithmischen Systems selbst, sondern die menschliche Letztentscheidung, die wegen Art. 22 DSGVO erforderlich ist.[6]

5. Bei einem nicht-lernenden System ist eine unmittelbare Benachteiligung denkbar, wenn z. B. bewusst bestimmte Gruppen beim Einprogrammieren der Entscheidungskriterien nicht berücksichtigt werden.[7]

6. Bei maschinell lernenden Systemen wird es eher zu mittelbaren Benachteiligungen kommen. Eine mittelbare Benachteiligung liegt gem. § 3 Abs. 2 AGG vor, wenn dem Anschein nach neutrale Vorschriften, Kriterien oder Verfahren Personen wegen eines in § 1 AGG genannten Grundes gegenüber anderen Personen in besonderer Weise benachteiligen. Die verwendeten Kriterien und Parameter des maschinell lernenden Systems ergeben sich aus der Auswertung der Trainingsdaten. Deshalb sind sie an sich neutral. Wegen unzutreffender Korrelationen können sich dennoch mittelbare Benachteiligungen ergeben.[8] Außerdem kann es sein, dass die Trainingsdatenqualität mangelhaft ist.[9]

7. Der Vorschlag von *Spiecker gen. Döhmann* und *Towfigh*, den Anwendungsbereich des § 1 AGG auch auf eine Benachteiligung zu erstrecken, die sich „aus einer Beziehung ergibt, die nur auf statistischer Korrelation beruht", überzeugt aus drei Gründen nicht.[10] Insbesondere fehlt einem solchen Benachteiligungsmerkmal der materielle Charakter der sonstigen in § 1 AGG genannten Merkmale, weil sich der Vorschlag

---

[6] Kapitel 9 A.II.1.a) (S. 296).
[7] S. Kapitel 8 B.III. (S. 290).
[8] Kapitel 8 B.II. (S. 289).
[9] Kapitel 8 B.I. (S. 288).
[10] Kapitel 9 A.II.1.b) (S. 298).

auf nicht auf den Entscheidungsgrund, sondern das Entscheidungsverfahren bezieht.

8. Gem. § 7 AGG muss die Benachteiligung *wegen* eines in § 1 AGG genannten Merkmals erfolgen (Kausalität).[11] Dabei reicht es aus, wenn die Benachteiligung wegen mehrerer Merkmale (sog. Motivbündel) erfolgt. Da maschinell lernende Systeme mit vielen Daten trainiert werden, wird die Benachteiligung typischerweise nicht nur auf einem Merkmal beruhen.[12]

9. Eine unmittelbare Benachteiligung kann im Einzelfall nach §§ 8-10 AGG gerechtfertigt sein. Wenn der Einsatz eines algorithmischen Systems eine positive Maßnahme i. S. d. § 5 AGG ist, kommt auch eine Rechtfertigung nach § 5 AGG in Betracht.

10. Eine mittelbare Benachteiligung ist gem. § 3 Abs. 1 Hs. 2 AGG gerechtfertigt, wenn die Vorschriften, Kriterien oder Verfahren, die zu einer mittelbaren Benachteiligung führen, durch ein rechtmäßiges Ziel sachlich gerechtfertigt und die Mittel zur Erreichung des Ziels angemessen und erforderlich sind. Die Arbeitgeberin verfolgt in aller Regel ein legitimes Ziel mit dem Einsatz des algorithmischen Systems.[13]

11. Auf der Ebene der Erforderlichkeit ist zu prüfen, ob es ein gleich geeignetes, milderes Mittel gegenüber dem Einsatz eines algorithmischen Systems gibt.[14] Herkömmliche Verfahren zur Auswahl von Personen sind – wie auch bereits im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO deutlich wird – nicht unbedingt milder gegenüber der Auswahl durch algorithmische Systeme. Das liegt daran, dass man je nach Vorgang des Auswahlprozesses bei algorithmischen Systemen die Möglichkeit hat, Probeläufe zu absolvieren.[15]

---

[11] Kapitel 9 A.II.1.c) (S. 298).
[12] Kapitel 9 A.II.2. (S. 301).
[13] Kapitel 9 A.III.2.a) (S. 304).
[14] Kapitel 9 A.III.2.b)bb) (S. 306).
[15] S. dazu bereits Kapitel 6 C.IV.2.c)aa) (S. 178).

12. Vorausgesetzt, es gibt kein gleich geeignetes, milderes Mittel, muss der Einsatz des algorithmischen Systems auch angemessen sein.[16] Das bedeutet, dass das System die legitimen Interessen der Personen nicht übermäßig beeinträchtigen darf, die wegen eines in § 1 AGG genannten Grundes mittelbar benachteiligt werden.

13. Im Rahmen der Angemessenheitsprüfung ist erstens zu berücksichtigen, dass es der Arbeitgeberin grundsätzlich zumutbar ist, die Kosten für ein qualitativ höherwertigeres und somit zu weniger Benachteiligungen führendes Trainingsdatenset aufzuwenden.[17] Wenn keine besseren Trainingsdaten verfügbar sind oder es mit unverhältnismäßigen Kosten verbunden wären, bessere Trainingsdaten zu beschaffen, ist das System zweitens nur angemessen, wenn die Arbeitgeberin nachweist, dass das eingesetzte System signifikant und nachweislich zu weniger voreingenommen Ergebnissen kommt als andere (nicht algorithmische) Verfahren.

14. Die Arbeitgeberin haftet bei Verstößen gegen das Benachteiligungsverbot nach § 15 Abs. 1 S. 1 AGG oder § 15 Abs. 2 S. 1 AGG. § 15 Abs. 1 AGG setzt ein Vertretenmüssen gem. §§ 276 ff. BGB seitens der Arbeitgeberin voraus (§ 15 Abs. 1 S. 2 AGG), für dessen Fehlen die Arbeitgeberin darlegungs- und beweispflichtig ist.[18] Beim Umfang des Vertretenmüssens ist zu berücksichtigen, welches Wissen die Arbeitgeberin über das algorithmische System hat.[19] Grundsätzlich muss sich die Arbeitgeberin nach den Grundsätzen der Wissenszurechnung das Wissen über den *Output* (Ergebnis des Systems) und teilweise auch über den *Input* (insbesondere die Trainingsdaten) zurechnen lassen.

15. Handelt die Herstellerin fahrlässig, wird das Verschulden der Herstellerin der Arbeitgeberin gem. § 278 S. 1 BGB zugerechnet.[20] Die

---

[16] Kapitel 9 A.III.2.b)cc) (S. 307).
[17] S. Kapitel 9 A.III.2.b)cc) (S. 307).
[18] Kapitel 9 B.I.1. (S. 310).
[19] S. Kapitel 9 B.I.1.a) (S. 311).
[20] Kapitel 9 B.I.1.b) (S. 314).

Arbeitgeberin hat gem. § 12 Abs. 1 AGG die Pflicht, Maßnahmen zum Schutz vor Benachteiligungen zu treffen. Das umfasst im Kontext algorithmischer Systeme auch, dass sie sicherstellen muss, dass keine diskriminierenden Parameter verwendet werden.

16. § 278 S. 1 BGB ist nicht analog auf algorithmische Systeme selbst anzuwenden, wenn die Ursache der Benachteiligung durch das System nicht auf menschliches Handeln der Herstellerin zurückgeführt werden kann. [21] Eine Regelungslücke besteht schon deshalb nicht, weil Arbeitgeberin und die Herstellerin das System auf eine mögliche mittelbare Benachteiligung hin überprüfen und entsprechende Vorkehrungen treffen müssen. Somit ist die Herstellerin Erfüllungsgehilfin i. S. d. § 278 S. 1 BGB.

17. Der Anspruch nach § 15 Abs. 1 S. 1 AGG scheitert in der Praxis fast immer, weil die Bewerberin nicht darlegen und beweisen kann, dass sie die am besten geeignete Kandidatin für die Position gewesen wäre. [22]

18. Relevanter ist daher der Anspruch auf angemessene Entschädigung nach § 15 Abs. 2 S. 1 AGG. [23] Die Anspruchstellerin muss im Schadensersatzprozess als nach den allgemeinen Grundsätzen darlegungs- und beweisbelastete Partei Indizien vortragen, die auf eine Benachteiligung i. S. d. AGG schließen lassen. Zwar statuiert § 22 AGG eine Beweiserleichterung: Beweist die eine Partei Indizien, die eine Benachteiligung wegen eines in § 1 AGG genannten Grundes vermuten lassen, trägt die andere Partei die Beweislast dafür, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligung vorgelegen hat. Diese wird bei algorithmischen Systemen aber kaum weiterhelfen, weil die Anspruchstellerin zumeist keinen näheren Einblick in das System hat. Damit § 22 AGG im Kontext algorithmischer Systeme

---

[21] Kapitel 9 B.I.2. (S. 316).
[22] Kapitel 9 B.I.3. (S. 318).
[23] Kapitel 9 B.II. (S. 318).

seinen Normzweck erfüllt, muss das von *Grünberger* entwickelte Zwei-Stufen-Modell der Darlegungslast greifen.[24]

[24] Kapitel 9 B.II.1.c) (S. 321).

Teil 4

Anforderungen aufgrund einer zukünftigen KI-VO

Wie bereits erwähnt worden ist[1], werden die in der Arbeit untersuchten Systeme in den Anwendungsbereich einer zukünftigen KI-VO fallen.

Daher wird im Folgenden untersucht, welche wesentlichen Vorgaben nach dem KI-VO-KOM, KI-VO-Rat und KI-VO-PARL für Hochrisiko-KI-Systeme gelten[2] und ob die Vorgaben der drei Entwürfe den Vorschriften der DSGVO widersprechen oder sie (sinnvoll) ergänzen[3]. Schließlich werden die wesentlichen Ergebnisse zusammengefasst.[4]

---

[1] Kapitel 5 A.IV.5. (S. 82).
[2] Kapitel 10 (S. 341).
[3] Kapitel 11 (S. 363).
[4] Kapitel 12 (S. 393).

Kapitel 10

Vorgaben für Hochrisiko-KI-Systeme

Der folgende Abschnitt enthält einen Überblick über die Akteurinnen[1] einer zukünftigen KI-VO sowie über die Anforderungen an Hochrisiko-KI-Systeme, die in Kapitel 2 des KI-VO-KOM geregelt sind.

Bei den Anforderungen an Hochrisiko-KI-Systeme liegt der Fokus auf den Vorgaben für die Trainingsdatenqualität und die Transparenzvorgaben nach Art. 13 KI-VO-KOM. Art. 10 KI-VO-KOM ist die erste Norm, die umfassend Qualitätsanforderungen für Trainingsdaten aufstellt.[2] Eine solche Norm ist angesichts der herausragenden Bedeutung der Qualität der Daten für algorithmische Systeme, wie bereits an einigen Stellen der Arbeit deutlich geworden ist[3], dringend geboten. Die Transparenzvorgaben sind entscheidend, weil das Vertrauen in KI-Systeme davon abhängt, wie transparent diese sind.[4]

A. Akteurinnen einer zukünftigen KI-VO

Der KI-VO-KOM kennt als Akteurinnen Anbieterinnen, Nutzerinnen, Bevollmächtigte, Einführerinnen und Händlerinnen (Art. 3 Nr. 7 KI-VO-KOM). Für den Untersuchungsgegenstand dieser Arbeit sind vor allem die Anbieterinnen und Nutzerinnen relevant, weil sich der KI-VO-KOM gem.

---

[1] Kapitel 10 A. (S. 341).

[2] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 53.

[3] S. etwa: Kapitel 6 C.IV.2.b)aa) (S.176); Kapitel 8 B. (S. 288).

[4] Kapitel 4 B.III. (S. 46).

Art. 2 Abs. 1 KI-VO-KOM vorrangig an Anbieterinnen und Nutzerinnen von KI-Systemen richtet.

Die Anbieterin ist in Art. 3 Nr. 2 KI-VO-KOM als Person definiert, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen. Anbieterin ist damit typischerweise die Entwicklerin, die das KI-System erstellt hat und es Dritten gegen Entgelt zur Verfügung stellt. Eine Arbeitgeberin, die ein KI-System einkauft, um es im eigenen Unternehmen zu nutzen, ist dagegen keine Anbieterin.

Nach Art. 28 Abs. 1 KI-VO-KOM unterliegen jedoch auch Dritte den Pflichten einer Anbieterin, wenn sie ein Hochrisiko-KI-System unter ihrem Namen oder ihrer Marke in Verkehr bringen oder in Betrieb nehmen. Das gleiche gilt, wenn Dritte die Zweckbestimmung eines bereits im Verkehr befindlichen Hochrisiko-KI-Systems verändern oder wenn sie eine wesentliche Änderung an einem Hochrisiko-KI-System vornehmen. Der KI-VO-PARL nimmt Änderungen am Wortlaut des Art. 28 Abs. 1 KI-VO-KOM vor, ändert dessen Wesensgehalt aber nicht. Eine Arbeitgeberin, die ein marktreifes KI-System einsetzt und dieses nicht modifizieren und nicht als eigenes System vermarkten möchte, fällt nicht unter Art. 28 Abs. 1 KI-VO-KOM. Sie ist somit keine Anbieterin und unterfällt daher nicht den Pflichten für Anbieterinnen nach Art. 16 KI-VO-KOM.

Nutzerin ist gem. Art. 2 Nr. 4 KI-VO-KOM eine Person, die ein KI-System in eigener Verantwortung zu beruflichen Zwecken verwendet. Dieser Begriff umfasst eine Arbeitgeberin, die ein KI-System eingekauft hat und es für Auswahlentscheidungen einsetzt. Im KI-VO-PARL wurde der Begriff der Nutzerin in den Begriff Bereitstellerin geändert.[5] Das ist sinnvoll, da es dann nicht zu Verwechselungen kommt, wenn man diejenigen Personen bezeichnen möchte, die ein KI-System als Endnutzerinnen direkt verwenden.[6]

---

[5] Report on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), A9-0188/2023, S. 119.

[6] *Haataja/Bryson*, AC 4 (2023), 707, 709.

Wenn z. B. ein Chatbot im Bewerbungsportal eingesetzt wird, wird man die Bewerberinnen, die mit dem Chatbot interagieren, typischerweise als Endnutzerinnen des KI-Systems verstehen. Nach der Definition in Art. 3 Nr. 4 KI-VO-KOM wäre aber die Arbeitgeberin die Nutzerin des Chatbots. Begriffstechnisch ist es vor diesem Hintergrund sinnvoller, dass die Arbeitgeberin nach Art. 3 Nr. 4 KI-VO-PARL Bereitstellerin ist. So kann man die Bewerberinnen im Beispiel als Nutzerinnen bezeichnen, ohne dass es zu Unklarheiten kommt.

Auch wenn im KI-VO-PARL der sachnähere Begriff der Bereitstellerin eingeführt wurde, wird der Begriff der Nutzerin indes weiter verwendet, obwohl er nicht mehr definiert wird. In Art. 13. Abs. 1 KI-VO-PARL werden z. B. sowohl Anbieterinnen also auch Nutzerinnen angesprochen. Die finale KI-VO sollte für alle drei Akteurinnen – Anbieterinnen, Bereitstellerinnen und Nutzerinnen – eine Definition bereithalten, damit man klar zwischen ihnen abgrenzen kann.

B. Überblick über die Anforderungen nach Kapitel 2 KI-VO-KOM

Die in Kapitel 2 KI-VO-KOM geregelten Anforderungen an Hochrisiko-KI-Systeme richten sich gem. Art. 16 KI-VO-KOM an die Anbieterinnen.

Sie müssen nach Art. 16 KI-VO-KOM unter anderem sicherstellen, dass die Systeme die Anforderungen des Kapitel 2 erfüllen (Art. 16 lit. a KI-VO-KOM).

Die Anbieterin muss ein Risikomanagementsystem einrichten, anwenden, dokumentieren und aufrechterhalten (Art. 9 Abs. 1 KI-VO-KOM). Das Risikomanagementsystem versteht sich als „kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems“ (Art. 9 Abs. 2 KI-VO-KOM). Dabei werden unter anderem die Risiken, die von einem Hochrisiko-KI-System ausgehen, ermittelt, analysiert, abgeschätzt und bewertet.

Nach Art. 11 KI-VO-KOM muss die Anbieterin bei Hochrisiko-KI-Systemen eine technische Dokumentation erstellen, die stets aktualisiert werden muss (Art. 11 Abs. 1 KI-VO-KOM). Aus der technischen Dokumentation muss der Nachweis hervorgehen, dass das Hochrisiko-KI-System die Anforderungen nach Kapitel 2 des KI-VO-KOM erfüllt. Den zuständigen Behörden und notifizierten Stellen müssen alle erforderlichen Informationen für die Beurteilung, ob die Anforderungen erfüllt sind, zur Verfügung stehen.

Hinzu kommen Aufzeichnungspflichten: Nach Art. 12 Abs. 1 KI-VO-KOM muss die Anbieterin alle Vorgänge und Ereignisse während des Betriebs automatisch aufzeichnen; die Funktionsweise des KI-Systems muss gem. Art. 12 Abs. 2 KI-VO-KOM in einem „der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar sein".

Hochrisiko-KI-Systeme müssen so entwickelt sein, dass sie während ihrer Verwendung von natürlichen Personen wirksam beaufsichtigt werden können (Art. 14 Abs. 1 KI-VO-KOM). Das soll die Risiken für Gesundheit, Sicherheit oder Grundrechte natürlicher Personen verhindern oder minimieren (Art. 14 Abs. 2 KI-VO-KOM). Schließlich müssen Hochrisiko-KI-Systeme im Hinblick auf ihre Zweckbestimmung genau, robust und cybersicher sein (Art. 15 Abs. 1 KI-VO-KOM). Art. 15 Abs. 1 lit. a und b KI-VO-PARL ergänzen, dass etwa das KI-Büro unter Mitarbeit bestimmter Behörden unverbindliche Leitlinien für die technischen Aspekte wie Genauigkeit, Robustheit und Cybersicherheit bereitstellt. Außerdem soll die Europäische Agentur für Cybersicherheit beim Europäischen Ausschuss für Künstliche Intelligenz (Art. 56 KI-VO-KOM) beteiligt werden, um neu auftretende Probleme des Binnenmarktes im Hinblick auf die Cybersicherheit zu behandeln. Es scheint ein Versehen zu sein, dass im KI-VO-PARL noch der Ausschuss für Künstliche Intelligenz erwähnt wird, da dieser Ausschuss im KI-VO-PARL durch das „KI-Büro" ersetzt wurde. Letzteres ist eine unabhängige Einrichtung der Union, die sich unter anderem um die Umsetzung der KI-VO kümmert und in dieser Hinsicht die Mitgliedstaaten und Aufsichtsbehörden unterstützt und berät (Art. 56 b KI-VO-PARL). Unabhängig von der Begrifflichkeit ist es eine Verbesserung gegenüber dem KI-VO-KOM und KI-VO-RAT, dass im KI-VO-PARL die Aufgaben des KI-Büros genauer präzisiert sind (Art. 56 b KI-VO-PARL).

I. Vorgaben für die Trainingsdatenqualität gem. Art. 10 Abs. 3, 4 KI-VO-KOM

Nach Art. 10 Abs. 3 KI-VO-KOM müssen die Trainings-, Test- und Validierungsdatensätze relevant, repräsentativ, vollständig und fehlerfrei sein.[7] Eine Definition dieser Merkmale liefert der KI-VO-KOM nicht.[8] In Art. 10 Abs. 3 KI-VO-PARL sind die Vorgaben nicht absolut gefasst, sondern einer Abwägung zugänglich. Die Trainingsdatensätze inklusive ihrer Label müssen relevant, *hinreichend* repräsentativ, *angemessen* auf Fehler *überprüft* und im Hinblick auf den beabsichtigten Zweck *so vollständig wie möglich* sein.[9]

Neben den Vorgaben des Art. 10 Abs. 3 KI-VO-KOM müssen die Trainingsdatensätze nach Art. 10 Abs. 4 KI-VO-KOM, soweit es für die Zweckbestimmung erforderlich ist, den Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind. Wenn ein System in der Personalauswahl in Deutschland eingesetzt wird, darf es etwa nicht anhand von Daten US-amerikanischer Bewerberinnen trainiert werden.[10] Art. 10 Abs. 4 KI-VO-PARL sieht neben der Bestimmung, dass es für den beabsichtigten Zweck des Systems erforderlich ist, vor, dass das KI-System auch den genannten Merkmalen oder Elementen entsprechen muss, wenn Missbrauch des KI-Systems vorhersehbar ist. Ob diese Erweiterung hilfreich ist, bleibt fragwürdig. Häufig wird erst die tatsächliche Anwendung des Systems zeigen, ob das KI-System missbraucht wird.

---

[7] Kritisch zu den Anforderungen s. *Bryson/Haataja*, Competition Policy International 14.03.2022, 5; *Bomhard/Merkle*, RDi 2021, 276, 280; *Linardatos*, GPR 2022, 58, 64; *Roos/Weitz*, MMR 2021, 844, 847; es wird nicht weiter zwischen Trainings-, Test- und Validierungsdatensätzen unterschieden, s. dazu bereits: Kapitel 1 C. Fn. 43.

[8] *Heil*, MPR 2022, 1, 9, die Art. 10 Abs. 3 KI-VO-KOM als Herausforderung für KI-basierte Medizinprodukte-Software sieht.

[9] Hervorhebung von der Verfasserin.

[10] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 60.

Zwar könnte man meinen, dass Anforderungen an die Datenqualität sich bereits aus Art. 5 DSGVO ergeben.[11] Personenbezogene Daten müssen etwa „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein" (Art. 5 Abs. 1 lit. d DSGVO). Außerdem müssen die personenbezogenen Daten gem. Art. 5 Abs. 1 lit. a DSGVO[12] auf rechtmäßige Weise, nach Treu und Glauben und für die betroffene Person in nachvollziehbarer Weise verarbeitet werden. Diese Vorgabe betrifft aber nicht die Datenqualität, sondern *wie* die Daten verarbeitet werden. Die Datenqualität bezieht sich hingegen darauf, *welche* Anforderungen die verarbeiteten Daten selbst haben. Die Vorgaben der DSGVO sind zudem nur anwendbar, wenn es sich um die Verarbeitung personenbezogener Daten handelt. Die Vorgaben des Art. 10 Abs. 3, 4 KI-VO-KOM sind hingegen allgemein für Trainingsdatensätze relevant, gleichwohl ob es sich um personenbezogene Daten handelt oder nicht.

1. Auslegung der Merkmale des Art. 10 Abs. 3 KI-VO-KOM

Ein für die Auslegung wichtiger Grundsatz geht aus Erwägungsgrund 44 KI-VO-KOM hervor. Dieser besagt, dass die Datensätze die Merkmale im „Hinblick auf die Zweckbestimmung des Systems" erfüllen müssen. Das bedeutet also, dass die Merkmale immer vor dem Hintergrund des konkreten Anwendungsfalls verstanden werden müssen. Je nach KI-System kann das jeweilige Merkmal unterschiedlich ausgelegt werden. Hinzu kommt, dass zu der Qualität von Daten bereits umfassend geforscht wird und klassische Dimensionen von Datenqualität in der Informatik bekannt sind.[13] Wie aus Erwägungsgrund 49 KI-VO-KOM hervorgeht, sollen Hochrisiko-KI-Systeme unter anderem ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit entsprechend dem allgemein anerkannten Stand der Technik aufweisen. Über die Formulierung „Stand der Technik" werden also auch technische Normen und Vorgaben berücksichtigt. Nichts anderes kann auch für Art. 10 Abs. 3 KI-VO-KOM gelten: Durch Art. 10 Abs. 3 KI-VO-KOM

---

[11] Zur Verbindlichkeit der Datenschutzgrundsätze s. Kapitel 6 A.IV. (S. 114).

[12] S. etwa bereits: Kapitel 4 (S. 39).

[13] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 54; *Heinrich/Klier*, in: Hildebrand/Gebauer/Mielke (Hrsg.), Daten- und Informationsqualität: die Grundlage der Digitalisierung, 5. Aufl. 2021, 52 ff.

wird gesetzlich normiert, dass bestimmte Qualitätsvorschriften auf Trainingsdaten zutreffen müssen.[14]

a) Relevanz

Das Merkmal der „relevanten" Datensätze ist in anderen Sprachfassungen gleichermaßen aufgeführt; die Sprachfassungen divergieren nicht. Das Adjektiv „relevant" wird im allgemeinen Sprachgebrauch als Synonym für bedeutsam, entscheidend oder ausschlaggebend verwendet.[15]

In systematischer Hinsicht kann man Art. 10 Abs. 2 lit. e KI-VO-KOM heranziehen, wonach die Datensätze vorher unter anderem daraufhin untersucht werden müssen, ob sie sich „eignen". Es sollten also nur relevante, d. h. geeignete und entscheidende Daten, die für den Zweck des Systems dienlich sind, als Trainingsdatensätze verarbeitet werden.

Der Regelungszweck der Norm ist unklar. Vermutlich soll mit dieser Vorgabe vermieden werden, dass viele Daten zu Trainingszwecken genutzt werden, die sich eigentlich gar nicht für den konkreten Trainingszweck eignen. Daten, die sich aber schon aus technischen oder anderen Gründen nicht zum Training des KI-Systems eignen, werden wohl kaum verarbeitet werden. Schließlich hängt von der Qualität der Daten die Qualität des Ergebnisses ab.[16] Auch die Vorgaben der DSGVO gelten weiterhin. Handelt es sich um personenbezogene Daten, müssen die Anforderungen der DSGVO gewahrt werden. Viele Daten zu verarbeiten, deren Verarbeitung nicht notwendig für den bestimmten Zweck ist, widerspricht Art. 5 Abs. 1 lit. c DSGVO.[17] Die Verarbeitung ist nur dann auf das *notwendige* Maß beschränkt, wenn nur

---

[14] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 62.

[15] S. https://perma.cc/JC3E-46UD (archiviert am 04.03.2023).

[16] *Lauscher/Legner*, ZfDR 2022, 367, 371; *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 53; *Kroll/Huey/Barocas u.a.*, Univ. Pa. Law Rev. 165 (2017), 633, 688; *Neutatz/Abedjan*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 1, 4; s. dazu auch: Kapitel 8 B.I. (S. 281).

[17] S. dazu unter: Kapitel 11 C. (S. 380).

relevante Daten für den konkreten Zweck verarbeitet werden. Das Merkmal der relevanten Daten ist somit gewissermaßen bereits in Art. 5 Abs. 1 lit. c DSGVO verankert.

Angesichts dessen bleibt unklar, inwiefern die Vorgabe des Art. 10 Abs. 3 KI-VO-KOM noch einen eigenen Regelungszweck erfüllt.

b) Repräsentativität

Auch für das Merkmal der „repräsentativen" Datensätze ergeben sich keine Anhaltspunkte durch den Vergleich der verschiedenen Sprachfassungen. Synonym für das Adjektiv „repräsentativ" werden die Begriffe charakteristisch, kennzeichnend, stellvertretend verwendet. [18] Systematisch kann abermals auf Art. 10 Abs. 2 KI-VO-KOM zurückgegriffen werden: Art. 10 Abs. 2 lit. c KI-VO-KOM verweist auch darauf, dass für die geeigneten Datensätze relevante Datenaufbereitungsvorgänge wie Kommentierung, Kennzeichnung, Bereinigung, Anreicherung und Aggregierung genutzt werden. Wenn Datensätze im Zuge der Anforderungen von Art. 10 Abs. 5 KI-VO-KOM bereinigt oder angereichert werden können, können Datensätze nur „repräsentativ" sein, wenn bei den charakteristischen Datenkategorien keine Benachteiligung angelegt ist. Zur Frage, wann eine Benachteiligung vorliegt, sollte man das AGG heranziehen. Auch wenn die im AGG genannten Kriterien nicht abschließend sind, so bietet das AGG zumindest einen ersten Anhaltspunkt. Die Daten sind auch dann nicht repräsentativ, wenn sie nicht zur Aufgabe passen, die das System lösen soll: Enthält etwa ein Datensatz aussagekräftige Daten für die Kreditwürdigkeit von Studentinnen, kann auf dieser Grundlage nicht die Kreditwürdigkeit von Pensionärinnen eingeschätzt werden.[19]

Verwendet man pseudonymisierte oder anonymisierte Daten, muss man ebenfalls darauf achten, dass diese Daten repräsentativ sind. Die Vorgaben für

---

[18] S. https://perma.cc/2ZGB-V5CA (archiviert am 04.03.2023).

[19] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 55.

personenbezogene und nicht personenbezogene Trainingsdaten sind nicht unterschiedlich.

c) Fehlerfreiheit

Außerdem müssen die Trainingsdatensätze gem. Art. 10 Abs. 3 KI-VO-KOM fehlerfrei sein. Im KI-VO-PARL wurde diese Voraussetzung in Art. 10 Abs. 3 KI-VO-PARL dahingehend geändert, dass die Trainingsdatensätze angemessen auf Fehler überprüft werden.

Bomhard und *Merkl*e schlagen vor, dass als mögliche Fehler z. B. durch fehlerhafte Sensoren hervorgerufene Mess- und Festplattenfehler (CRC-Fehler) in Betracht kommen.[20] Ein solches Verständnis deckt aber nicht alle möglichen Fehlertypen ab. In der Forschung zu Datenqualität wird unter Fehlerfreiheit etwa die Eigenschaft verstanden, dass „die im Informationssystem abgelegten Werte mit den tatsächlichen, realen Werten übereinstimmen"[21]. Anders formuliert sind Daten dann fehlerfrei, wenn keine sachlich unzutreffenden Informationen im System hinterlegt sind, etwa das falsche Geschlecht. Dieses Verständnis der Fehlerfreiheit muss auch bei Art. 10 Abs. 3 KI-VO-KOM zugrunde gelegt werden. Art. 10 Abs. 3 KI-VO-KOM ist gegenüber dem Grundsatz der Datenrichtigkeit gem. Art. 5 Abs. 1 lit. d DSGVO – sofern dieser überhaupt anwendbar ist – *lex specialis*.[22] Insofern kann man die grundsätzlichen Wertungen des Art. 5 Abs. 1 lit. d DSGVO auch heranziehen, der auch auf „sachlich richtige" Daten abstellt.

Das Merkmal ist aber aus zwei Gründen problematisch. Wie auch bei den anderen Merkmalen setzt das Merkmal der Fehlerfreiheit voraus, dass die Daten bereits vor dem Training dieser Anforderung gerecht werden. Das ist aber insofern praktisch schwierig, weil zunächst mit einer Vielzahl an Daten

---

[20] *Bomhard/Merkle*, RDi 2021, 276, 280.

[21] *Heinrich/Klier*, in: Hildebrand/Gebauer/Mielke (Hrsg.), Daten- und Informationsqualität: die Grundlage der Digitalisierung, 5. Aufl. 2021, 55; *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 54, die den Begriff „Richtigkeit" wählen, aber i. E. dasselbe meinen.

[22] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 59.

trainiert und erst auf zweiter Ebene ein „Fine-Tuning" stattfindet. Mit den Vorgaben für die Trainingsdatenqualität setzt die KI-VO aber vor dem Training an und setzt damit voraus, dass man schon genau abschätzen kann, welche Daten man für das Training benötigt und wie diese Daten im Hinblick auf den Zweck geeignet sind.

Außerdem bleibt unklar, was genau Fehlerfreiheit bedeutet. Ob ein Datum keinen „Fehler" wie etwa Mess- und Festplattenfehler aufweist und ob das Datum sachlich richtig ist, kann man nicht anhand eines konkreten Einzeldatums feststellen.

d) Vollständigkeit

Vollständigkeit muss vor dem Hintergrund, dass Daten auch im Hinblick auf mögliche Verzerrungen untersucht werden sollen, so ausgelegt werden, dass Daten von z. B. allen ethnischen Gruppen in einem Datensatz abgebildet sind, um etwaigen Benachteiligungen vorzubeugen. Es ist nahezu unmöglich, einen „vollständigen" Datensatz als Trainingsdatensatz für algorithmische Systeme zu haben.[23] Man könnte Datensätze somit als vollständig einstufen, wenn sie keine Verzerrungen hervorrufen. Es wird aber kaum möglich sein, ein System mit derartigen Datensätzen zu erstellen. *Linardatos* legt das Merkmal wie folgt aus: Ein System werde mit einem vollständigen Datensatz trainiert, wenn es alle „offensichtlich notwendigen Werte und Parameter für die Berechnung eines Umweltzustands" enthalte: [24] Man müsse etwa einem Steueralgorithmus Zugang zu den Wetterdaten verschaffen, weil er das Lenkverhalten ansonsten nicht an die Umweltbedingungen anpassen könne. In der Forschung zu Datenqualität wird das Merkmal der Vollständigkeit wie folgt verstanden: Die im Informationssystem hinterlegten Attribute müssen mit einem Wert versehen sein. [25] Das würde bedeuten, dass ein Datensatz vollständig i. S. d. Art. 10 Abs. 3 KI-VO-KOM ist, wenn für die erfassten

[23] *Grützmacher*, CR 2021, 433, 440; *Heil*, MPR 2022, 1, 9; *Veale/Borgesius*, Computer Law Review International 22 (2021), 97, 103.

[24] *Linardatos*, GPR 2022, 58, 64, Fn. 76.

[25] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 54; *Heinrich/Klier*, in: Hildebrand/Gebauer/Mielke (Hrsg.), Daten- und Informationsqualität: die Grundlage der Digitalisierung, 5. Aufl. 2021, 52.

Bestandteile der Daten auch jeweils Werte vorliegen, etwa die Dauer der Betriebszugehörigkeit. Soll aber ein algorithmisches System die für eine höhere Position geeignete Arbeitnehmerin finden, braucht es neben der Dauer der Betriebszugehörigkeit etwa noch Daten über die Produktivität der Arbeitnehmerinnen. Es muss mithin auch bei der Auswahl der *Datenkategorien* auf Vollständigkeit geachtet werden. Im Rahmen von Art. 10 Abs. 3 KI-VO-KOM muss das Merkmal der Vollständigkeit daher weiter verstanden werden als die soeben vorgestellte Definition: Ein Datensatz ist vollständig, wenn das algorithmische System alle notwendigen Datenkategorien abbildet, um ein bestimmtes Ergebnis zu präsentieren. Im Unterschied dazu meint das Merkmal der Repräsentativität, dass innerhalb dieser Datenkategorien Diversität herrscht, also insbesondere keine Benachteiligung nach dem AGG angelegt ist[26].

e) Geeignete statistische Merkmale

Außerdem sieht Art. 10 Abs. 3 S. 2 KI-VO-KOM vor, dass die Trainingsdatensätze geeignete statistische Merkmale aufweisen, gegebenenfalls auch bezüglich der Personen oder Personengruppen, für die das Hochrisiko-KI-System bestimmungsgemäß eingesetzt werden soll. Der Datensatz muss mithin im Hinblick auf verschiedene geschützte Gruppen ausgewogen sein.[27] Wenn ein Hautkrebs-Erkennungssystem in einer ethnisch diversen Bevölkerungsgruppe eingesetzt wird, müssen die Daten die unterschiedlichen Schattierungen von Hautfarben abbilden. [28] Aus dem Merkmal „bestimmungsgemäße Verwendung" lässt sich schließen, dass es weniger darum geht, eine Balance zwischen allen möglichen denkbar geschützten Gruppen herzustellen, sondern vielmehr, darauf zu achten, dass der Datensatz gruppenspezifisch repräsentativ ist.[29]

---

[26] Kapitel 10 B.I.1.b) (S. 348).

[27] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 60 f.

[28] *Dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 61 m. w. N.

[29] *Dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 61.

Insbesondere vor dem Hintergrund des Merkmals der Repräsentativität, welches bereits sicherstellen soll, dass der Datensatz gruppenspezifisch ausgewogen ist und keine Benachteiligung nach AGG angelegt ist, ist der eigene Regelungszweck von Art. 10 Abs. 3 S. 2 KI-VO-KOM fraglich. Eine Unterscheidung kann man darin sehen, dass bei Art. 10 Abs. 3 S. 2 KI-VO-KOM der konkrete Einsatzbereich des Hochrisiko-KI-Systems im Fokus steht, wohingegen es beim Merkmal der Repräsentativität darauf nicht vorrangig ankommt. Es wird allerdings kaum möglich sein, den Datensatz ohne den konkreten Einsatzbereich auszuwählen.

2. Handhabbare Umsetzung in der Praxis durch Art. 10 Abs. 3 KI-VO-PARL

Wie kann man nun garantieren, dass Nutzerinnen und Anbieterinnen ihre KI-Systeme mit Datensätzen trainieren, testen und validieren, die die genannten Merkmale erfüllen? *Linardatos* schlägt vor, dass die Anbieterinnen entsprechenden Transparenz- und Nachweispflichten nachkommen sollten. Man könnte einen Privilegierungstatbestand nach dem Vorbild des § 1 Abs. 2 Nr. 5 ProdHaftG in die künftige KI-VO aufnehmen. Nach § 1 Abs. 2 Nr. 5 ProdHaftG ist eine Ersatzpflicht der Herstellerin ausgeschlossen, wenn der Fehler nach dem Stand der Wissenschaft und Technik zu dem Zeitpunkt, zu dem die Herstellerin das Produkt in den Verkehr gebracht hat, nicht erkannt werden konnte.

Ähnlich formuliert *Linardatos* einen möglichen Tatbestand für das Merkmal der Fehlerhaftigkeit: „Trainings-, Validierungs- und Testdaten gelten nicht als fehlerhaft, wenn etwaige Mängel, Lücken oder Verzerrungen nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt der Inverkehrgabe oder Inbetriebnahme nicht erkannt werden konnten.“ [30] Eine weitere Herausforderung ist dabei gleichermaßen, welchen Stand der Wissenschaft und Technik man genau zu welchem Zeitpunkt zugrunde legt. [31] Der Ausschuss für KI, der unter anderem die nationalen Aufsichtsbehörden und die Kommission dabei unterstützt, die einheitliche Anwendung der Verordnung zu gewährleisten (Art. 56 Abs. 2 lit. c KI-VO-KOM), soll auch im

---

[30] *Linardatos*, GPR 2022, 58, 65; ähnlich auch: *Lücke*, Recht und Politik 2021, 52.

[31] In einem anderen Kontext, aber zu dem ähnlichen Problem s. *Weidenhammer/Gundlach*, DuD 2018, 106.

Hinblick auf den Stand der Wissenschaft und Technik den Überblick behalten und zu diesen Fragen beraten.

Hacker und *Wessel* schlagen hingegen vor, dass es Toleranzbereiche geben sollte, innerhalb derer je nach Risikoträchtigkeit des KI-Systems davon ausgegangen werden kann, dass die Anforderungen an die Datenqualität noch gewahrt sind.[32] Außerdem müsse es möglich sein, dass man Datensätze im Hinblick darauf modifiziere, dass die Privatsphäre der betroffenen Personen stärker geschützt werde, auch wenn dies zu einer höheren Fehlerquote führen sollte.[33] Auf die weiteren regulatorischen Ansätze soll an dieser Stelle aber nicht vertieft eingegangen werden.[34]

Die Vorschläge überzeugen. Der Vorschlag von *Linardatos* setzt daran an, dass die Herstellerin oder Verwenderin des KI-Systems umfassende Dokumentations- und Nachweispflichten erfüllen muss, um die Konformität ihres Systems nachzuweisen. Das verhindert in der Praxis eine doppelte Arbeit, da gem. Art. 11 KI-VO-KOM ohnehin eine technische Dokumentation erstellt werden muss. In dieser Dokumentation muss auch festgehalten werden, ob die Trainingsdaten die Anforderungen nach Art. 10 Abs. 3 KI-VO-KOM erfüllen. Allerdings sollten in einer solchen Regelung, wie sie *Linardatos* vorschlägt, alle möglichen Qualitätskriterien aufgeführt werden. Die Trainingsdaten sollten nicht nur als fehlerfrei gelten, wenn sie die Anforderungen an den Stand der Wissenschaft und Technik genügen, sondern nur dann, wenn sie auch relevant, repräsentativ und vollständig sind. Die von *Hacker* und *Wessel* vorgeschlagenen Toleranzbereiche sind notwendig: Bei großen Datensätzen sind gewisse „Fehler, Leerstellen und Imperfektionen [...] unvermeidbar."[35] Deshalb sind Art. 10 Abs. 3 KI-VO-PARL sowie Art. 10 Abs. 3 KI-VO-RAT sehr zu begrüßen. Der Wortlaut des

---

[32] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 65.

[33] *Dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 65.

[34] *Dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 65 ff.

[35] *Dies.*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 65.

Art. 10 Abs. 3 KI-VO-RAT lautet: „Die Trainings-, Validierungs- und Testdatensätze müssen relevant, repräsentativ und *so weit wie möglich* [36] fehlerfrei und vollständig sein." Die Vorgaben in Art. 10 Abs. 3 KI-VO-PARL sind gegenüber Art. 10 Abs. 3 KI-VO-RAT noch offener formuliert: Die Trainingsdatensätze und gegebenenfalls die Validierungs- und Testdatensätze, einschließlich der Kennzeichnungen, müssen relevant, *hinreichend* repräsentativ, *angemessen* auf Fehler *überprüft* und im Hinblick auf den beabsichtigten Zweck so vollständig wie möglich sein. Sie müssen die geeigneten statistischen Eigenschaften aufweisen, gegebenenfalls auch in Bezug auf die Personen oder Personengruppen, für die das KI-System für hohe Risiken eingesetzt werden solle. Diese Merkmale der Datensätze müssen auf der Ebene der einzelnen Datensätze oder einer Kombination davon erfüllt sein.

Dennoch zeigen die obigen Ausführungen, dass die Anforderungen trotz abwägungsoffener Formulierung nur schwierig zu erfüllen sind. [37] Insbesondere ist ein Aspekt entscheidend: Aus Sicht der zukünftigen KI-VO müssen die Voraussetzungen für das Trainingsdatenset erfüllt sein, bevor das System trainiert wird. Es ist schwierig, schon vorher abzuschätzen, ob die Daten für den entsprechenden Trainingszweck die genannten Merkmale erfüllen. Letztlich führen die Vorgaben für Trainingsdaten aber dazu, dass ungeprüfte, große Datensätze nicht einfach zum Training von KI-Systemen verwendet werden dürfen. Gerade angesichts möglicher Diskriminierungen, die durch unzureichende Trainingsdatensätze hervorgerufen werden können[38], ist eine Regelung für die Anforderungen an Trainingsdaten richtig und wichtig. Mit Inkrafttreten der Regelung sollte gleichermaßen auch der Umgang mit geprüften Datensätzen gefördert werden.[39]

---

[36] Hervorhebung von der Verfasserin.

[37] S. dazu: *Müller-Peltzer/Tanczik*, RDi 2023, 452, 457.

[38] S. Kapitel 8 A. (S. 281).

[39] Ein positives Beispiel s. etwa: https://perma.cc/3R2C-69SF (archiviert am 06.07.2023); s. dazu auch: *Bundesregierung*, Strategie Künstliche Intelligenz der Bundesregierung, 2018, S. 35.

II. Transparenz i. S. d. Art. 13 KI-VO-KOM und KI-VO-PARL

1. Vorgaben des Art. 13 KI-VO-KOM

Anbieterinnen müssen Hochrisiko-KI-Systeme in einer Weise konzipieren und entwickeln, dass sie transparent betrieben werden, damit die Nutzerinnen die Ergebnisse des Systems angemessen interpretieren und verwenden können (Art. 13 Abs. 1 KI-VO-KOM). Die Transparenz soll gem. Art. 13 Abs. 1 S. 2 KI-VO-KOM auf eine geeignete Art und in einem angemessenen Maß gewährleistet werden, damit die Nutzerinnen und Anbieterinnen ihre in Kapitel 3 des KI-VO-KOM festgelegten einschlägigen Pflichten erfüllen können. Weitere Transparenzpflichten für bestimmte KI-Systeme regelt Art. 52 KI-VO-KOM[40]: Handelt es sich etwa um ein System, das Emotionen erkennt, müssen die betroffenen Personen über den Betrieb des Systems vorab informiert werden. Diese Transparenzpflicht ist aber gegenüber Art. 13 Abs. 1 KI-VO-KOM nicht weitergehender, sondern hat nach dem zugrundeliegenden Verständnis dieser Arbeit vor allem klarstellende Bedeutung.

Wie bereits herausgearbeitet worden ist, wird Transparenz in dieser Arbeit als Oberbegriff für die Nachvollziehbarkeit und Erklärbarkeit verwendet.[41] Dass man Ergebnisse „angemessen interpretieren" kann, setzt voraus, dass man das Ergebnis des Systems nachvollziehen und im konkreten Kontext auch erklären kann. Zwar kann man aufgrund der technischen Umstände – wie z. B. bei den verschiedenen Schichten eines neuronalen Netzes[42] – die Funktionsweise von KI-Systemen kaum vollständig nachvollziehen.[43] Allerdings schränkt das Wort „angemessen" die Transparenzpflichten auch dahingehend ein, dass die Nutzerinnen nicht umfassend informiert werden müssen. Vielmehr müssen sie in der Lage sein, das Ergebnis in seinem Kontext zu sehen und die richtigen Schlüsse daraus zu ziehen.

---

[40] S. im Kurzüberblick dazu: *Günther-Burmeister*, DB 2021, 1858, 1862.

[41] Kapitel 4 B. (S. 44).

[42] Kapitel 1 C.II.1. (S. 18).

[43] Kapitel 4 A.I.1. (S. 40); s. im Kontext von Art. 13 KI-VO-KOM auch *Bomhard/Merkle*, RDi 2021, 276, 280, die eine Nachvollziehbarkeit von KI-Systemen derzeit kaum für möglich halten.

Inhaltlich kann man sich am Umfang der Informationspflicht nach Art. 13 Abs. 2 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO orientieren.[44] Der verfolgte Zweck von Art. 13 Abs. 1 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO und Art. 13 Abs. 1 KI-VO-KOM ist derselbe: Es müssen bestimmte Informationen über das System verfügbar sein, um das Ergebnis des Systems angemessen verwenden oder interpretieren zu können. Nach Art. 13 Abs. 1 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO hat die betroffene Person das Recht, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erhalten. Die involvierte Logik meint die grundsätzliche Funktionsweise des Algorithmus bzw. Systems sowie die relevanten Parameter.[45] In Bezug auf die Tragweite sowie Auswirkungen der Verarbeitung muss die Person darüber in Kenntnis gesetzt werden, welche möglichen Auswirkungen die Verarbeitung auf ihre Grundrechte hat und welche Schutzmaßnahmen für ihre personenbezogenen Daten ergriffen werden.[46] Diese Maßstäbe sollten auch im Rahmen von Art. 13 Abs. 1 KI-VO-KOM zugrunde gelegt werden.

2. Definition von Transparenz in Art. 13 Abs. 1 KI-VO-PARL

Nach Art. 13 Abs. 1 KI-VO-PARL sollen Hochrisiko-KI-Systeme hingegen von den Anbieterinnen so konzipiert und entwickelt werden, dass Anbieterinnen selbst und Nutzerinnen *einigermaßen verstehen können*, wie das System funktioniert.

Konkretisiert wird dieses Transparenzverständnis durch die in Art. 13 Abs. 1 KI-VO-PARL enthaltene Definition des Begriffs Transparenz. Demnach bedeutet Transparenz i. S. d. Art. 13 Abs. 1 KI-VO-PARL, dass zum Zeitpunkt des Inverkehrbringens des Hochrisiko-KI-Systems alle nach dem allgemein anerkannten Stand der Technik verfügbaren technischen Mittel eingesetzt werden, um sicherzustellen, dass die Ergebnisse des KI-Systems für die Anbieter- und die Nutzerinnen interpretierbar sind. Sie müssen in die Lage versetzt werden, das KI-System zu verstehen und angemessen zu nutzen,

---

[44] Kapitel 7 B.III.1. (S. 267).
[45] Kapitel 7 B.III.1.a) (S. 250).
[46] Kapitel 7 B.III.2. (S. 253).

indem sie allgemein wissen, wie das KI-System funktioniert und welche Daten es verarbeitet, so dass sie den betroffenen Personen gemäß Art. 68c KI-VO-PARL[47] die vom KI-System getroffenen Entscheidungen erklären können. Diese Definition konkretisiert Art. 4a Abs. 1 lit. d KI-VO-PARL, wonach Transparenz bedeutet, dass das KI-System stets so entwickelt und verwendet werden muss, dass es angemessen nachvollziehbar und erklärbar ist. Außerdem muss den betroffenen Personen bewusst sein, dass sie mit einem KI-System kommunizieren und interagieren. Schließlich müssen die Nutzerinnen über die Fähigkeiten und Grenzen des KI-Systems sowie die betroffenen Personen über ihre Rechte ordnungsgemäß informiert werden.

Im Unterschied zu Art. 13 Abs. 1 KI-VO-KOM ist die Ausweitung auf Anbieterinnen sinnvoll. Schließlich müssen nicht nur die Nutzerinnen, sondern auch die Anbieterinnen selbst hinreichendes Verständnis über das System haben. Die Vorgaben des Art. 13 Abs. 1 KI-VO-PARL unterscheiden sich inhaltlich nur unwesentlich von Art. 13 Abs. 1 KI-VO-KOM, sodass – wie bereits ausgeführt – die Inhalte der Informationspflichten nach Art. 13 Abs. 1 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO herangezogen werden sollten.[48] Trotz der Vorgaben des Art. 13 Abs. 1 KI-VO-KOM oder KI-VO-PARL bleibt es das Wesen eines Hochrisiko-KI-Systems, dass die Erklärbarkeit nicht einfach umgesetzt werden kann:[49] Auch für die Herstellerinnen des KI-Systems selbst ist es mitunter nicht erklärbar, wie ein Ergebnis zustande gekommen ist.

C. Ausgestaltung der Vorschriften und Rechtsfolgen bei Nichteinhaltung

Die Anforderungen an Hochrisiko-KI-Systeme sind als „Muss-Vorschriften“ ausgestaltet.[50] Die Hochrisiko-KI-Systeme *müssen* die in Kapitel 2 festgelegten Anforderungen erfüllen (Art. 8 Abs. 1 KI-VO-KOM). Auch

---

[47] S. dazu: Kapitel 11 F. (S. 386).

[48] Kapitel 7 B.III. (S. 250).

[49] Vgl. Kapitel 1 C.II. (S.17); Kapitel 4 A. (S. 40).

[50] S. zu „Kann-Vorschriften“ und „Soll-Vorschriften“ *Wank*, Juristische Methodenlehre, 2020, § 7 Rn. 117 ff.

müssen Anbieterinnen den Pflichten nach Art. 16 lit. a-j KI-VO-KOM nachkommen.

Nach Art. 71 Abs. 1 KI-VO-KOM sollen die Mitgliedstaaten entsprechend des KI-VO-KOM Vorschriften für Sanktionen erlassen.

Der KI-VO-KOM enthält konkrete Vorgaben für die Sanktionen. Für die Höhe der Geldbuße werden gem. Art. 71 Abs. 6 KI-VO-KOM die Art, Schwere und Dauer des Verstoßes und dessen Folgen (Art. 71 Abs. 6 lit. a KI-VO-KOM) berücksichtigt. Außerdem wird geprüft, ob bereits andere Marktüberwachungsbehörden derselben Akteurin für denselben Verstoß Bußgelder auferlegt haben (Art. 71 Abs. 6 lit. b KI-VO-KOM). Schließlich werden Größe und Marktanteil der Akteurin, die den Verstoß begangen hat, berücksichtigt (Art. 71 Abs. 6 lit. c KI-VO-KOM). Art. 71 Abs. 6 KI-VO-PARL nennt zudem die Möglichkeit, dass zusätzlich zu oder anstelle von Bußgeldern nichtmonetäre Maßnahmen wie Anordnungen oder Verwarnungen verhängt werden können.

Ist ein KI-System etwa nicht konform mit den Vorgaben an die Trainingsdaten gem. den in Art. 10 KI-VO-KOM festgelegten Anforderungen, werden Bußgelder von bis zu 30.000.000 EUR oder – im Fall von Unternehmen – von bis zu 6 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist (Art. 71 Abs. 3 KI-VO-KOM). Art. 71 Abs. 3 KI-VO-RAT ergänzt, dass sich die Bußgelder auf bis zu 3% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs belaufen, wenn es sich um KMU (kleine und mittlere Unternehmen) einschließlich Start-Up-Unternehmen handelt. Im KI-VO-PARL wird die Höhe bei einem Verstoß gegen Art. 10 KI-VO-PARL auf 20.000.000 EUR oder 4% vom gesamten weltweiten Jahresumsatz heruntergesetzt.

D. Zwischenergebnis zu den Vorgaben der Hochrisiko-KI-Systeme

1. Der KI-VO-KOM richtet sich gem. Art. 2 Abs. 1 KI-VO-KOM an Anbieterinnen und Nutzerinnen, [51] wobei die meisten Pflichten Anbieterinnen treffen. Anbieterin ist eine Person, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen. Darunter fällt typischerweise die Entwicklerin des KI-Systems. Die Arbeitgeberin, die das KI-System im eigenen Unternehmen einsetzt, ist hingegen keine Anbieterin, sondern regelmäßig die Nutzerin gem. Art. 2 Nr. 4 KI-VO-KOM, weil sie das KI-System nicht modifizieren und als eigenes System vermarkten möchte.

2. Der Begriff der Nutzerin wird im KI-VO-PARL sinnvollerweise in den Begriff Bereitstellerin geändert. [52] So kommt es nicht zu Verwechselungen, wenn man diejenigen Personen bezeichnen möchte, die ein KI-System als Endnutzerinnen direkt verwenden. Im KI-VO-PARL wird jedoch der Begriff der Nutzerin weiter verwendet, obwohl er nicht mehr definiert wird. Die finale KI-VO sollte für alle drei Akteurinnen – Anbieterinnen, Bereitstellerinnen und Nutzerinnen – eine Definition bereithalten, damit man zwischen den drei Begriffen eindeutig abgrenzen kann.

3. Anbieterinnen von Hochrisiko-KI-Systemen müssen die Anforderungen des Kapitel 2 KI-VO-KOM erfüllen. [53] Dazu gehört unter anderem, dass sie ein Risikomanagementsystem einrichten, anwenden, dokumentieren und aufrechterhalten müssen. Außerdem müssen sie eine technische Dokumentation erstellen, aus der der Nachweis hervorgeht, dass das Hochrisiko-KI-System die Anforderungen an Kapitel 2 des KI-VO-KOM erfüllt sowie dafür

---

[51] Kapitel 5 A.IV.3.b) (S. 79); Kapitel 10 A. (S. 341).
[52] Kapitel 10 A. (S. 341).
[53] Kapitel 10 B. (S. 343).

sorgen, dass das System während der Verwendung von natürlichen Personen wirksam beaufsichtigt werden kann.

4. Außerdem müssen die Trainings-, Test- und Validierungsdatensätze den Anforderungen nach Art. 10 Abs. 2 bis 5 KI-VO-KOM genügen.[54] Gem. Art. 10 Abs. 3 KI-VO-KOM müssen die Trainingsdaten *relevant, repräsentativ, fehlerfrei* und *vollständig* sein. Nach dem Wortlaut des Art. 10 Abs. 3 KI-VO-PARL ändert sich an den vier Merkmalen nichts; allerdings sind diese gemäß Art. 10 Abs. 3 KI-VO-PARL – anders als im KI-VO-KOM – sinnvollerweise einer Abwägung zugänglich: Die Trainingsdaten müssen relevant, *hinreichend repräsentativ*, *angemessen auf Fehler überprüft* und im Hinblick auf den beabsichtigten Zweck *so vollständig wie möglich* sein. Trotz abwägungsoffener Formulierung werden die Vorgaben nur schwierig zu erfüllen sein. Das liegt vor allem daran, dass die Voraussetzungen für das Trainingsdatenset erfüllt sein müssen, *bevor* das System trainiert wird. Es ist schwierig, schon im Voraus abzuschätzen, ob die Daten die genannten Merkmale für den entsprechenden Trainingszweck erfüllen. Allerdings wird durch eine solche Regelung aber jedenfalls verhindert, dass ungeprüfte, große Datensätze zum Training von KI-Systemen genutzt werden. Mit Inkrafttreten der Regelung wird somit der Umgang mit geprüften Datensätzen gefördert. Das ist richtig und wichtig, da unzureichende Trainingsdatensätze Benachteiligungen hervorrufen können.[55]

5. Das Merkmal der *relevanten Datensätze* muss so verstanden werden, dass vermieden werden soll, dass viele Daten zu Trainingszwecken genutzt werden, die an sich nicht für den Trainingszweck geeignet sind.[56] Der eigene Regelungszweck des Merkmals ist unklar, weil Daten, die sich aus technischen oder anderen Gründen nicht zum Training des KI-Systems eignen, ohnehin nicht verarbeitet werden. Handelt es sich um personenbezogene Daten, muss ohnehin der Grundsatz der Datenminimierung gem. Art. 5 Abs 1 lit. c DSGVO eingehalten werden. Demnach dürfen ohnehin nur relevante Daten für den

[54] Kapitel 10 B.I. (S. 345).
[55] Vgl. Kapitel 8 (S. 281).
[56] Kapitel 10 B.I.1.a) (S. 347).

konkreten Zweck verarbeitet werden, weil die Verarbeitung ansonsten nicht auf das notwendige Maß gem. Art. 5 Abs. 1 lit. c DSGVO beschränkt wäre.

6. Trainingsdaten sind dann *repräsentativ*, wenn bei den für das Training charakteristischen Datenkategorien keine Benachteiligungen angelegt sind.[57] Als Anhaltspunkt für den Begriff der Benachteiligung sollte man das AGG heranziehen. Die im AGG aufgeführten Benachteiligungen sind allerdings nicht abschließend. Bei pseudonymisierten und anonymisierten Daten muss man ebenfalls darauf achten, dass die Daten repräsentativ sind. Für derartigen Daten gelten keine anderen Anforderungen.

7. Ein Datensatz ist *vollständig,* wenn das algorithmische System alle notwendigen Datenkategorien abbildet, um ein bestimmtes Ergebnis zu präsentieren.[58] Möchte man mithilfe eines algorithmischen Systems eine geeignete Arbeitnehmerin für eine höhere Position finden, benötigt man etwa neben der Dauer der Betriebszugehörigkeit noch Aussagen über die Produktivität der Arbeitnehmerinnen. Im Unterscheid dazu ist vom Merkmal der Repräsentativität erfasst, dass innerhalb dieser Datenkategorien Diversität gewährleistet ist, also insbesondere keine Benachteiligung nach dem AGG vorliegt.

8. Beim Merkmal der *Fehlerfreiheit* bleibt unklar, was genau Fehlerfreiheit bedeutet. [59] Ob ein Datum keinen „Fehler“ wie etwa Mess- und Festplattenfehler aufweist und ob es sachlich richtig ist, ist nicht anhand eines konkreten Einzeldatums feststellbar. Außerdem ist das Merkmal problematisch, weil man vor dem Training häufig nicht genau abschätzen kann, welche Daten man konkret für das Training des algorithmischen Systems benötigt. Das „Fine-Tuning“ findet erst auf der zweiten Ebene statt.

---

[57] Kapitel 10 B.I.1.b) (S. 348).
[58] Kapitel 10 B.I.1.d) (S. 350).
[59] Kapitel 10 B.I.1.c) (S. 349).

9. Der eigene Regelungszweck der Vorgabe des Art. 10 Abs. 3 S. 2 KI-VO-KOM, nach dem die Trainingsdatensätze geeignete statistische Merkmale aufweisen müssen, ist fraglich.[60] Bereits nach dem Merkmal der Repräsentativität der Datensätze müssen Nutzerinnen und Anbieterinnen sicherstellen, dass der Datensatz gruppenspezifisch ausgewogen ist und keine Benachteiligung nach dem AGG angelegt ist. Eine Unterscheidung kann man darin sehen, dass bei Art. 10 Abs. 3 S. 2 KI-VO-KOM der konkrete Einsatzbereich des Hochrisiko-KI-Systems im Fokus steht, wohingegen es beim Merkmal der Repräsentativität darauf nicht vorrangig ankommt. Allerdings wird es kaum möglich sein, den Datensatz ohne den konkreten Einsatzbereich auszuwählen.

10. Art. 13 Abs. 1 KI-VO-KOM regelt, dass Anbieterinnen ihr Hochrisiko-KI-System in einer Weise konzipieren und entwickeln müssen, dass es transparent betrieben wird, damit die Nutzerinnen die Ergebnisse des Systems angemessen interpretieren und verwenden können. Dabei sollten die inhaltlichen Maßstäbe der Informationspflicht nach Art. 13 Abs. 2 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO gelten[61], weil der verfolgte Zweck identisch ist. In beiden Fällen müssen bestimmte Informationen über das System vorliegen, um das Ergebnis des Systems angemessen verwenden oder interpretieren zu können.

11. Sinnvoll ist es, dass Art. 13 Abs. 1 KI-VO-PARL den Anwendungsbereich auf Anbieterinnen ausweitet. Nicht nur die Nutzerinnen, sondern auch die Anbieterinnen selbst müssen ein hinreichendes Verständnis des Systems haben.

12. Die Anforderungen an Hochrisiko-KI-Systeme sind als „Muss-Vorschriften“ ausgestaltet.[62] Sind die Anforderungen nicht erfüllt, werden Geldbußen verhängt.

---

[60] Kapitel 10 B.I.1.e) (S. 351).
[61] Kapitel 7 B.III.1. (S. 267).
[62] Kapitel 10 C. (S. 357).

Kapitel 11

KI-VO-KOM und DSGVO: Widerspruch oder (sinnvolle) Ergänzung?

Ausweislich der Begründung des KI-VO-KOM soll die DSGVO unberührt bleiben.[1] Durch die spezifischen Vorschriften für Entwurf, Entwicklung und Verwendung bestimmter Hochrisiko-KI-Systeme wird die DSGVO lediglich ergänzt. [2] Werden personenbezogene Daten mithilfe von KI-Systemen verarbeitet, ergeben sich jedoch Überschneidungen zur DSGVO, die nun erläutert werden. Vom KI-VO-KOM unbeantwortet bleibt, wie Überschneidungen im Hinblick auf die Vorgaben der DSGVO aufzulösen sind. Widersprechen sich DSGVO und KI-VO-KOM an bestimmten Stellen oder ergänzt der KI-VO-KOM die Vorgaben aus der DSGVO sinnvoll? Welche Aussagen trifft der KI-VO-PARL hinsichtlich des Verhältnisses zur DSGVO?

A. Zusammenspiel verschiedener Risikobewertungen und DSFA

I. Art. 9 KI-VO-KOM

Die Verantwortliche muss gem. Art. 35 DSGVO eine DSFA[3] durchführen, wenn eine Form der Verarbeitung ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen durch den Einsatz neuer

---

[1] Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM (2021) 206 final, S. 4.

[2] Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM (2021) 206 final, S. 4.

[3] Kapitel 7 A. (S. 241).

Technologien zur Folge hat. Bei algorithmischen Systemen, die bei der Personalauswahl und im Arbeitsverhältnis eingesetzt werden, wird eine DSFA in aller Regel erforderlich sein.[4] Ein solches System unterfällt – wie oben aufgezeigt[5] – der Kategorie der Hochrisiko-KI-Systeme, sodass die Anbieterin nach Art. 9 KI-VO-KOM i. V. m. Art. 16 Abs. 1 KI-VO-KOM ein Risikomanagementsystem einrichten, anwenden, dokumentieren und aufrechterhalten muss.

Die folgende Tabelle stellt Art. 35 DSGVO und Art. 9 KI-VO-KOM in Auszügen gegenüber:

[4] S. dazu: Kapitel 7 A. (S. 241).
[5] Kapitel 5 A.IV.5. (S. 82).

Art. 35 DSGVO	Art. 9 KI-VO-KOM
(7) Die Folgenabschätzung enthält zumindest Folgendes:	(2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:
a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;	a) Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;
b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;	b) Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird[6];
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und	c) Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.	d) Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.

[6] Im KI-VO-RAT und KI-VO-PARL entfällt Art. 9 Abs. 2 lit. b, im Übrigen ändert sich der Wesensgehalt von Art. 9 KI-VO-KOM aber nicht.

Die Gegenüberstellung zeigt: Im Kern enthalten Art. 9 Abs. 2 KI-VO-KOM und Art. 35 Abs. 7 DSGVO ähnliche Mindestvorgaben. Bei der DSFA geht es aber um eine Risikobewertung der *Verarbeitung personenbezogener Daten.* Darauf kommt es beim Risikomanagementsystem nicht an: Es muss lediglich ein *Hochrisiko-KI-System* vorliegen. Die DSFA enthält neben einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung, einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck und einer Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen, auch die zur Bewältigung der Risiken von geplanten Abhilfemaßnahmen (Art. 35 Abs. 7 lit. a-d DSGVO). Im Rahmen des Risikomanagementsystems soll die Anbieterin demgegenüber insbesondere ermitteln und analysieren, welche bekannten und vorhersehbaren Risiken von einem Hochrisiko-KI-System ausgehen (Art. 9 Abs. 2 lit. a KI-VO-KOM).

Während die DSFA zeitlich stattfindet, *bevor* die personenbezogenen Daten verarbeitet werden, ist das Risikomanagementsystem als *kontinuierlicher* Prozess während des gesamten Lebenszyklus des KI-Systems zu verstehen.

Ein gewichtiger Unterschied zwischen der Pflicht zur Durchführung einer DSFA einerseits und der Pflicht zur Einrichtung und Aufrechterhaltung eines Risikomanagementsystems andererseits liegt darin, dass sie sich an unterschiedliche Akteurinnen richten. Die DSFA muss die datenschutzrechtlich Verantwortliche i. S. v. Art. 4 Nr. 7 DSGVO durchführen. Die Pflicht, ein Risikomanagementsystem einzurichten, anzuwenden, zu dokumentieren und aufrechtzuerhalten betrifft dagegen nach dem Einleitungssatz des Art. 16 lit. a KI-VO-KOM die Anbieterin. Wie oben bereits herausgearbeitet wurde, ist eine Arbeitgeberin typischerweise nicht die Anbieterin eines KI-Systems, sondern lediglich dessen Nutzerin i. S. v. Art. 2 Nr. 4 KI-VO-KOM bzw. dessen Bereitstellerin i. S. v. Art. 2 Nr. 4 KI-VO-PARL.

Wenn die Anbieterin eines KI-Systems bei dessen Erstellung personenbezogene Trainingsdaten verwendet, ist sie auch Verantwortliche i. S. d. DSGVO und muss somit sowohl ein Risikomanagementsystem

einrichten als auch eine DSFA durchführen.[7] Während die Pflicht zur Einrichtung des Risikomanagementsystems kontinuierlich gilt, greift die Pflicht zur Durchführung der DSFA ein, sobald eine Verarbeitung personenbezogener Daten stattfinden soll. Bevor es dazu kommt, muss die DSFA durchgeführt werden. Eine DSFA wäre nur nicht erforderlich, wenn der Anwendungsbereich der DSGVO nicht eröffnet wäre, also anonymisierte Daten verarbeitet werden.[8] Bei den untersuchten Systemen wird es indes i. d. R. nicht zielführend sein, die entsprechenden Daten zu anonymisieren, sodass die DSGVO anwendbar ist.[9] Sind daher sowohl eine DSFA als auch ein Risikomanagementsystem erforderlich, finden jeweils ähnliche Erwägungen im Rahmen der Risikobewertung und der geplanten Abhilfemaßnahmen statt. Die Risikobewertung bezieht sich nach der DSFA zwar auf Rechte und Freiheiten der betroffenen Person. Die vorhersehbaren Risiken, die im Risikomanagementsystem zu berücksichtigen sind, betreffen aber typischerweise insbesondere die Rechte und Freiheiten betroffener Personen. Man könnte daher überlegen, dass es möglich sein muss, innerhalb der DSFA auf die im Kontext des Risikomanagementsystems getroffenen Erwägungen zu verweisen, damit Synergieeffekte genutzt werden.

Die Arbeitgeberin, die das fertige System einsetzt, ist dagegen typischerweise lediglich Verantwortliche und muss „nur" eine DSFA durchführen. Zu dem Zeitpunkt, in dem die Arbeitgeberin das System einsetzt, wird es typischerweise schon eine von der Anbieterin für die Trainingsdaten durchgeführte DSFA und ein von der Anbieterin eingerichtetes Risikomanagementsystem geben. Auf diese Ressourcen kann die Arbeitgeberin für die eigene DSFA zurückgreifen. Darauf wird sie faktisch angewiesen sein, weil nur die Anbieterin, die das KI-System entwickelt hat, hinreichenden technischen Sachverstand hat. Anbieterin und Arbeitgeberin werden sich in der Regel auch vertraglich einigen, dass die Anbieterin die Arbeitgeberin bei der Durchführung der DSFA unterstützt. Ohne das Wissen der Anbieterin über Details des Hochrisiko-KI-Systems wird eine DSFA nicht umsetzbar sein. Man könnte daher überlegen, von vornherein die Anbieterin dazu zu verpflichten, eine DSFA durchzuführen, soweit andere

---

[7] S. dazu: Kapitel 6 B. (S. 117).

[8] Vgl. dazu: Kapitel 5 A.III.2.a)aa) (S. 65); Kapitel 6 B. (S. 117).

[9] Kapitel 6 B.I. (S. 118).

Verantwortliche ihr KI-System zur Datenverarbeitung einsetzen. Allerdings ist es keine KI-spezifische Herausforderung, eine DSFA durchzuführen. Auch bei anderen Anwendungsbereichen, wie etwa beim Einsatz von Office-Anwendungen, muss eine DSFA durchgeführt werden, und zwar von der Verantwortlichen, die die Office-Anwendungen einsetzt, nicht aber von der Herstellerin der Software. Es ist eine Grundentscheidung in der Systematik der DSGVO, dass Pflichten sich primär an Verantwortliche richten. Diese Systematik hat die KI-VO nicht durchbrochen. Mit Blick auf das obige Beispiel einer Office-Anwendung wäre eine solche Durchbrechung auch nicht sinnvoll gewesen. Es ist typisch, dass sich Verantwortliche beim Einsatz von Software in datenschutzrechtlicher und technischer Hinsicht von Spezialistinnen beraten lassen müssen. Das ist auch nach der Systematik des KI-VO-KOM nach wie vor möglich. Obwohl ein Austausch zwischen Verantwortlicher und Anbieterin somit möglich und in vielen Fällen hilfreich ist, zeigen die Ausführungen, dass die Pflicht, eine DSFA durchzuführen sowie die Pflicht, ein Risikomanagementsystem nach Art. 9 Abs. 1 KI-VO-KOM einzurichten und zu unterhalten, nicht vermischt werden sollten.

Außerdem zeigt die Regelung des Art. 9 Abs. 9 KI-VO-PARL, dass bestimmte Risikomanagementverfahren miteinander kombiniert werden können. Anders als bei Art. 29a KI-VO-PARL und Art. 54 Abs. 1 lit. c KI-VO-PARL (dazu sogleich) wird Art. 35 DSGVO in Art. 9 Abs. 9 KI-VO-PARL aber nicht erwähnt. Das Parlament hat mithin gesehen, dass Synergieeffekte mit verschiedenen Risikoerwägungen genutzt werden können; es hat sich aber beim Risikomanagementsystem nach Art. 9 KI-VO-PARL bewusst dazu entschieden, die DSFA nicht zu nennen.

II. Art. 29a KI-VO-PARL und Art. 35 DSGVO

Art. 29a KI-VO-PARL regelt, dass Bereitstellerinnen für die meisten Hochrisiko-KI-Systeme eine grundrechtliche Folgenabschätzung vornehmen müssen. Ausgenommen sind KI-Systeme, die in Annex III Bereich 2 genannt sind. Darauf soll an dieser Stelle nicht vertieft eingegangen werden.

In der Folgenabschätzung sollen gem. Art. 29a Abs. 1 KI-VO-PARL unter anderem der Zweck, für den das Hochrisiko-KI-System eingesetzt werden soll, und der räumliche und zeitliche Anwendungsbereich des Hochrisiko-KI-

Systems berücksichtigt werden. Außerdem soll Folgendes beachtet werden: die Kategorien betroffener natürlicher Personen und Gruppen; die voraussichtlichen Auswirkungen auf die Grundrechte, die dadurch entstehen, dass das Hochrisiko-KI-System eingesetzt wird und wie die Risiken abgeschwächt werden können. Wenn ein Plan, die Risiken abzuschwächen, nicht identifiziert werden kann, soll die Betreiberin das Hochrisiko-KI-System nicht benutzen.

Art. 29a Abs. 3-5 KI-VO-PARL regeln, wie mit der Folgenabschätzung umgegangen wird, wenn ein neues Hochrisiko-KI-System eingesetzt wird, welche betroffenen Personen und Aufsichtsbehörden man informieren soll und welche Regelungen greifen, wenn die Bereitstellerin eine Behörde oder ein Unternehmen im Sinne von Art. 51 Abs. 1a lit. b KI-VO-PARL ist.

Art. 29a Abs. 6 KI-VO-PARL enthält folgende Regelung: Wenn die Bereitstellerin bereits verpflichtet ist, eine DSFA gem. Art. 35 DSGVO durchzuführen, soll die grundrechtliche Folgenabschätzung in Zusammenhang mit der DSFA durchgeführt werden. Die DSFA soll als Anhang der grundrechtlichen Folgenabschätzung nach Art. 29a KI-VO-PARL veröffentlicht werden.

Es überzeugt, dass im Rahmen der grundrechtlichen Folgenabschätzung auf die DSFA verwiesen werden kann. Zum einen richten sich beide Pflichten regelmäßig an dieselbe Person: Die Arbeitgeberin wird Bereitstellerin i. S. d. Art. 3 Nr. 4 KI-VO-PARL sein; sie ist aber ebenfalls auch Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO.[10] Anders als das Risikomanagementsystem ist die grundrechtliche Folgenabschätzung ebenso wie die DSFA zunächst eine Maßnahme, die vor dem Einsatz des Hochrisiko-KI-Systems und vor der Verarbeitung der personenbezogenen Daten einmalig vorgenommen und – jedenfalls bei nur unwesentlichen Änderungen – nicht ständig aktualisiert werden muss. Zum anderen wird sich die grundrechtliche Folgenabschätzung nach Art. 29a KI-VO-PARL sowie nach Art. 35 DSGVO inhaltlich wenig unterscheiden: Es spielt sowohl im Rahmen der Folgenabschätzung nach Art. 29a KI-VO-PARL als auch im Rahmen der Folgenabschätzung nach

[10] Kapitel 10 A. (S. 341).

Art. 35 DSGVO eine Rolle, dass ein Hochrisiko-KI-System personenbezogene Daten verarbeitet.

III. Art. 54 Abs. 1 lit. c KI-VO-PARL und Art. 35 DSGVO

Nach Art. 53 Abs. 1 KI-VO-PARL richten die Mitgliedstaaten auf nationaler Ebene mindestens eine „*regulatory sandbox*" für KI-Regulierung ein, die spätestens am Tag des Inkrafttretens dieser Verordnung betriebsbereit sein muss. Unter einer „*regulatory sandbox*" versteht der KI-VO-PARL eine von einer Behörde eingerichtete und kontrollierte Umgebung, die die sichere Entwicklung, Erprobung und Validierung innovativer KI-Systeme für eine begrenzte Zeit vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem bestimmten Plan unter behördlicher Aufsicht ermöglicht (Art. 4 Abs. 1 Nr. 44g KI-VO-PARL).

Art. 54 KI-VO-KOM, KI-VO-RAT und KI-VO-KOM enthalten Vorgaben für die Verarbeitung von Daten in der „*regulatory sandbox*". Unter anderem sieht Art. 54 Abs. 1 lit. c KI-VO-PARL vor, dass es effektive Überwachungsmechanismen gibt, ob während der *Sandbox*-Experimente hohe Risiken für die Rechte und Freiheiten der betroffenen Personen auftreten können. Anders als der KI-VO-KOM erwähnen Art. 54 Abs. 1 lit. c KI-VO-RAT und KI-VO-PARL, dass mit diesen Risiken für die Rechte und Freiheiten der betroffenen Personen diejenigen Risiken gemeint sind, die gem. Art. 35 DSGVO oder Art. 35 DSVO[11] identifiziert wurden. Diese Erwägung ist zutreffend: Auch in diesem Hinblick ergeben sich Synergieeffekte zwischen einer Maßnahme nach einer zukünftigen KI-VO und der DSFA. In der „*regulatory sandbox*" sollen die Risiken überwacht werden, die dank der DSFA identifiziert worden sind.

IV. Zwischenergebnis: Gleichlauf der Pflichten nach einer zukünftigen KI-VO und der DSGVO nicht immer sinnvoll

1. Die Ausführungen zeigen, dass die in der DSFA vorgenommenen Erwägungen zu den Risiken, die für die Rechte und Freiheiten natürlicher Personen aufgrund der Form der Verarbeitung bestehen,

[11] Abl. L 295 vom 21.11.2018, S. 39.

auch in anderen Risikobewertungen relevant werden. Richtigerweise können Synergieeffekte aber nicht bei allen Maßnahmen nach einer zukünftigen KI-VO und Art. 35 DSGVO genutzt werden. Die Pflicht, ein Risikomanagementsystem nach Art. 9 KI-VO-KOM einzurichten und aufrechtzuerhalten betrifft die Anbieterin, mithin also typischerweise die Entwicklerin des Hochrisiko-KI-Systems. [12] Die verantwortliche Arbeitgeberin wird das Risikomanagementsystem nicht betreiben können, weil ihr das KI-spezifische Wissen regelmäßig fehlen wird. Sie wird deshalb die DSFA auch häufig nur mithilfe der Entwicklerin vornehmen können. Allerdings ist es keine KI-spezifische Herausforderung, eine DSFA vorzunehmen. Grundsätzlich ist es eine richtige Wertung einer zukünftigen KI-VO und der DSGVO, dass jeweils unterschiedliche Akteurinnen von den Pflichten betroffen sind.

2. Die Erwägungen, die in der DSFA getroffen wurden, können aber im Hinblick auf andere Pflichten nach einer zukünftigen KI-VO genutzt werden. Anders als der KI-VO-KOM und der KI-VO-RAT verweist der KI-VO-PARL in Art. 29a Abs. 6 und Art. 54 Abs. 1 lit. c KI-VO-PARL zurecht auf Art. 35 DSGVO.

B. (K)eine Überschneidung mit Art. 9 DSGVO?

Art. 10 Abs. 5 KI-VO-KOM regelt, dass Anbieterinnen personenbezogene Daten gem. Art. 9 Abs. 1 der DSGVO verarbeiten dürfen, „soweit dies für die Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist“. [13] Dabei müssen die Anbieterinnen „angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen“. Erfasst sind nach der Norm etwa Methoden wie Pseudonymisierung oder Verschlüsselung.

Art. 10 Abs. 5 KI-VO-PARL enthält deutlich strengere Einschränkungen. Hervorzuheben ist, dass sensible Daten nach Art. 9 Abs. 1 DSGVO nur

[12] Kapitel 10 A. (S. 341).
[13] Vgl. *Hornung*, DuD 2022, 561, 562 f.

verarbeitet werden dürfen, wenn die Erkennung und Korrektur von Verzerrungen nicht wirksam durch die Verarbeitung synthetischer oder anonymisierter Daten erfüllt werden kann (Art. 10 Abs. 5 S. 1 lit. a KI-VO-PARL). Die Anforderungen an die Erforderlichkeit der Verarbeitung sind mithin sehr hoch. Gem. Art. 10 Abs. 5 a. E. KI-VO-PARL muss zudem dokumentiert werden, warum die Verarbeitung sensibler Daten notwendig war, um Verzerrungen zu erkennen und zu verhindern. Wenn synthetische oder anonymisierte Daten nicht verwendet werden können, müssen die Daten pseudonymisiert werden (Art. 10 Abs. 5 S. 2 lit. b KI-VO-PARL). Es besteht mithin eine Pflicht zur Pseudonymisierung. Schließlich dürfen die Daten, die für Zwecke des Art. 10 Abs. 5 KI-VO-KOM und Art. 10 Abs. 5 KI-VO-PARL verarbeitet werden, nicht übermittelt, weitergegeben oder anderen Parteien zugänglich gemacht werden. Das schränkt auch eine Übermittlung im Konzern ein.

I. Regelungsgehalt von Art. 10 Abs. 5 KI-VO-KOM

Unklar ist, welchen Regelungsgehalt Art. 10 Abs. 5 KI-VO-KOM hat. Was versteht man unter „Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen"?[14] Verzerrungen werden gleichgesetzt mit dem englischen Begriff „*bias*" (Art. 10 Abs. 2 lit. f KI-VO-KOM), der in der Forschung eine deutlich stärkere Verbreitung aufweist als die deutsche Übersetzung. Eine feststehende Definition für *bias* im Kontext von KI-Systemen gibt es nicht.[15] In einer interdisziplinären Untersuchung zu „Bias in data-driven artificial intelligence systems"[16] wird *bias* definiert als „ inclination or prejudice of a decision made by an AI system which is for or against one person or group, especially in a way considered to be unfair"[17]. Gemeint sind also voreingenommene KI-Systeme, die solche Entscheidungen treffen, die als ungerecht wahrgenommen werden.

---

[14] *Ebers/Hoch/Rosenkranz u.a.*, RDi 2021, 528, 533; *Hornung*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 91, 103; *Lauscher/Legner*, ZfDR 2022, 367, 385; *Santos*, ZfDR 2023, 23-41, 33 ff.

[15] Kritisch dazu s. *Lauscher/Legner*, ZfDR 2022, 367, 385.

[16] *Ntoutsi/Fafalios/Gadiraju u.a.*, Bias in data-driven artificial intelligence systems – An introductory survey, 2020.

[17] *Dies.*, Bias in data-driven artificial intelligence systems – An introductory survey, 2020, S. 3 ff.

Lopez bezieht sich auf die Definition von *Friedman* und *Nissenbaum*, die ein Computersystem als voreingenommen betrachten, wenn es unfair und systematisch diskriminiert.[18] *Friedmann* und *Nissenbaum* differenzieren nach dem Ursprung des *bias* und unterteilen in *technical bias*, *pre-existing bias* und *emergent bias*.[19] *Technical bias* resultiere aus technischen Einschränkungen, *pre-existing bias* resultiere aus bestehenden Praktiken und Haltungen. *Emergent bias* entstehe im Zusammenhang mit der konkreten Nutzung des Systems.[20] Diese Form von Verzerrung trete typischerweise erst nach einiger Zeit auf, etwa wenn sich das Wissen der Gesellschaft oder bestimmter Gruppen änderten. Beispielsweise sei ein System ungeeignet, wenn es Wissen voraussetze, das die Nutzerinnen nicht hätten.[21] Das sei z. B. der Fall, wenn ein System vor allem schriftliche Anweisungen verwende, die Gruppe der Nutzerinnen aber überwiegend nicht der schriftlichen Sprache mächtig sei.[22]

Bereits nach dem geltenden EU-Recht ist nicht in jeder Hinsicht klar, welche Benachteiligungen verboten sind. Eine umfassende von der Kommission in Auftrag gegebene Untersuchung aus dem Jahr 2021 zeigt, dass „Ungereimtheiten, Mehrdeutigkeiten und Mängel im EU-Antidiskriminierungsrecht bestehen, sodass auch algorithmische Diskriminierungen in der Folge nicht rechtssicher erfasst werden können“[23]. Auch hilft ein Blick in das AGG nicht weiter: Der Begriff *bias* knüpft nicht an den im AGG gewählten Begriff der Benachteiligung an. Fallen gerechtfertigte Benachteiligungen nicht unter den Begriff des *bias*? Oder geht der Begriff sogar noch über den der Benachteiligung nach dem AGG hinaus? Das bleibt

---

[18] *Lopez*, Internet Policy Review 10 (2021), 1, 3 mit Verweis auf *Friedman/Nissenbaum*, ACM Transactions on Information Systems 1996, 330.

[19] *Friedman/Nissenbaum*, ACM Transactions on Information Systems 1996, 330, 332; *Lopez*, Internet Policy Review 10 (2021), 1, 3.

[20] *Friedman/Nissenbaum*, ACM Transactions on Information Systems 1996, 330, 332.

[21] *Dies.*, ACM Transactions on Information Systems 1996, 330, 335.

[22] *Dies.*, ACM Transactions on Information Systems 1996, 330, 335.

[23] *Gerards/Xenidis*, Algorithmic discrimination in Europe, 2021, S. 75; zu fehlenden Zielformulierungen im Hinblick auf Art. 14 IV KI-VO-KOM s. *Ebers/Hoch/Rosenkranz u.a.*, RDi 2021, 528, 534.

offen. [24] Man muss das Merkmal daher näher definieren, damit der Anwendungsbereich von Art. 10 Abs. 5 KI-VO-KOM einheitlich verstanden wird.

Vor obigem Hintergrund sollte unter *bias* i. S. d. Art. 10 Abs. 5 KI-VO-KOM grundsätzlich eine diskriminierende oder sonst benachteiligende Entscheidung gegenüber einer Person durch ein KI-System verstanden werden. Das Merkmal ist weit auszulegen und erfasst grundsätzlich jede Form der Benachteiligung. Man sollte sich an den Fallgruppen des AGG orientieren, die aber nicht abschließend verstanden werden sollten. Mögliche Verzerrungen in KI-Systemen sollten nicht nur dann erfasst werden, wenn sie im AGG genannt sind. Es können dabei alle Formen von *technical bias*, *pre-existing bias* und *emergent bias* erfasst sein. Diese Kategorien können helfen, die unterschiedlichen *biases* einzuordnen. Sie haben aber keinen weiteren Inhaltsbezug.

Auch gerechtfertigte Benachteiligungen sollten als *bias* eingestuft werden, weil die Frage der Rechtfertigung eine nachgelagerte Frage ist. Bei Art. 10 Abs. 5 KI-VO-KOM geht es aber darum, Verzerrungen an sich zu erkennen und zu korrigieren. Die Frage der Rechtfertigung einer Verzerrung spielt dabei noch keine Rolle. Für die gegenteilige Auffassung, dass nur ungerechtfertigte Benachteiligungen als Verzerrung eingestuft werden sollten, spricht Art. 10 Abs. 5 KI-VO-PARL. Der Begriff *bias* wurde gegenüber Art. 10 Abs. 5 KI-VO-KOM in *negative bias* geändert. *Negative bias* könnte sich dem Wortlaut nach nur auf ungerechtfertigte Benachteiligungen beziehen. Allerdings ist auch der Zweck von Art. 10 Abs. 5 KI-VO-PARL, Verzerrungen zu bekämpfen. Dafür muss man zunächst alles beobachten und sollte nicht nur *negative biases* erfassen. Die Konkretisierung von *negative bias* im KI-VO-PARL ist keine Verbesserung, sondern schafft mehr Unklarheiten. Was genau unter *negative bias* und im Umkehrschluss unter *positive bias* verstanden wird, ist ungeklärt.

---

[24] Kritisch dazu s. *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 63; *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt, S. 66.

II. Ausnahme nach Art. 9 Abs. 2 lit. g DSGVO

Art. 9 Abs. 1 DSGVO statuiert ein Verbot der Verarbeitung sensibler Daten. Geklärt werden muss, wie sich dieses Verbot auf Art. 10 Abs. 5 KI-VO-KOM auswirkt. Es könnte die Ausnahme des Art. 9 Abs. 2 lit. g DSGVO einschlägig sein. Art. 9 Abs. 2 lit. g DSGVO ist eine horizontale Öffnungsklausel [25]: Gem. Art. 9 Abs. 1 lit. g DSVGO gilt Art. 9 Abs. 1 DSGVO nicht, wenn die Verarbeitung auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

Die erforderliche Grundlage des Unionsrechts ist Art. 10 Abs. 5 KI-VO-KOM. Dieser Artikel dient dem Ziel der Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen. Vorgesehen ist, dass angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten getroffen werden. Die erste Voraussetzung des Art. 9 Abs. 2 lit. g DSGVO ist mithin erfüllt.

Zudem muss ein erhebliches öffentliches Interesse vorliegen. Ein solches öffentliches Interesse an der Verarbeitung liegt vor, wenn sie Gemeininteressen dient.[26] Die Verarbeitung dient Gemeininteressen, wenn es um die Durchsetzung der Rechtsstaatlichkeit, der Gefahrenabwehr, der Strafverfolgung oder der Wahrung von Gleichheit und Solidarität geht.[27] Um Verzerrungen zu verhindern oder jedenfalls abzuschwächen, müssen gem. Art. 10 Abs. 5 KI-VO-KOM besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DSGVO verarbeitet werden. Ansonsten können Benachteiligungen hervorgerufen oder verstärkt werden. Wenn man personenbezogene Daten verarbeitet, müssen auch sensible Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden. Wenn ein KI-System etwa wegen des Geschlechts diskriminiert, müssen logischerweise auch gerade solche Daten

---

[25] Gola/Heckmann/*Schulz*, Art. 9 DSGVO Rn. 37.

[26] Kühling/Buchner/*Weichert*, Art. 9 DSGVO Rn. 90.

[27] Kühling/Buchner/*ders.*, Art. 9 DSGVO Rn. 90; vgl. *Hilgers*, ZD 2020, 556, 559.

verarbeitet werden, um Diskriminierungen zu verhindern. Die Gleichbehandlung dient Gemeininteressen, sodass die Voraussetzung eines öffentlichen Interesses erfüllt ist.

Das öffentliche Interesse muss auch erheblich sein.[28] Es muss also gewichtige Gründe für die Verarbeitung sensibler Daten geben. Im Bereich der Gefahrenabwehr kann das etwa ein hochrangiges, besonders schützenswertes Rechtsgut sein.[29] § 22 Abs. 1 Nr. 1 lit. c BDSG, der auf Grundlage des Art. 9 Abs. 2 lit. g DSGVO erlassen wurde, benennt verschiedene erhebliche öffentliche Interessen, z. B. die öffentliche Gesundheit.[30] Eine entsprechende Aufzählung enthält Art. 10 Abs. 5 KI-VO-KOM nicht. Dennoch schützt die Norm faktisch öffentliche Interessen, da das Gebot der Nichtdiskriminierung, das auch in Art. 21 GRCh verankert ist, ein öffentliches Interesse ist. Die Verhinderung von *biases* dient nicht nur einzelnen Personen, sondern ist ein gesamtgesellschaftliches Interesse. Der Ursprung von Diskriminierung liegt schließlich nicht beim Individuum selbst, sondern vielmehr sind die Strukturen und der Kontext, in dem das Individuum agiert, Ausgangspunkt für die Diskriminierung.[31]

Im Ergebnis liegen somit die Voraussetzungen von Art. 9 Abs. 2 lit. g DSGVO vor. Art. 10 Abs. 5 KI-VO-KOM steht mithin nicht im Widerspruch zu Art. 9 Abs. 1 DSGVO.

III. Eigenständige Rechtsgrundlage?

Neben einem Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO ist für die Rechtmäßigkeit der Datenverarbeitung zusätzlich erforderlich, dass eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegt.[32] Art. 10 Abs. 5 KI-VO-KOM ist keine eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Das geht aus Erwägungsgrund 41 KI-VO-KOM

---

[28] Zweifelnd *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188, 1190.

[29] Kühling/Buchner/*Weichert*, Art. 9 DSGVO Rn. 91.

[30] Kühling/Buchner/*ders.*, Art. 9 DSGVO Rn. 91.

[31] *Beigang/Fetz/Kalkum u.a., S.* 13.

[32] *BT-Drs. 18/11325*, S. 94; vgl. zu § 22 BDSG, der auf Grundlage des Art. 9 Abs. 2 lit. g DSGVO beruht: Gola/Heckmann/*Heckmann/Scheurer*, § 22 BDSG Rn. 6; Kapitel 6 A.II.1.b) (S. 105).

hervor: „Diese Verordnung sollte nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bildet, auch nicht für besondere Kategorien personenbezogener Daten." Der BVMed sieht in dieser Aussage einen Widerspruch zu Art. 10 Abs. 5 KI-VO-KOM. Art. 10 Abs. 5 KI-VO-KOM sei nicht als Rechtsgrundverweisung formuliert, weshalb aus der Norm nicht hervorgehe, dass auch eine zusätzliche Rechtsgrundlage erforderlich sei.[33] Führt man den Gedanken weiter, ist Art. 10 Abs. 5 KI-VO-KOM nach der Ansicht des BVMed als Rechtsgrundlage zu verstehen.

Für eine solche Einordnung spricht nunmehr auch Erwägungsgrund 41 KI-VO-PARL. Der ursprünglich enthaltene Satz, dass diese Verordnung nicht so verstanden werden sollte, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bildet, ist in Erwägungsgrund 41 KI-VO-PARL nicht mehr enthalten.

Das ist überzeugend. 10 Abs. 5 KI-VO-KOM sieht enge Einschränkungen für die Datenverarbeitung vor. Es wäre reiner Formalismus, zusätzlich auch noch eine Abwägung nach Art. 6 Abs. 1 lit. f DSGVO zu verlangen. Für diese wäre dann eine weitere Dokumentation – neben den vielen Dokumentationspflichten, die es ohnehin schon gibt – erforderlich. Es ist kein sinnvoller Regelungsansatz, andere Regulierungen immer unberührt zu lassen. Stattdessen sollten Doppelstrukturen in der Regulierung nach Möglichkeit reduziert werden, damit sie nicht immer komplizierter wird. Sichergestellt werden muss, dass die Anforderungen nach Art. 9 Abs. 2 DSGVO gewahrt sind, weil nur in diesen engen Ausnahmefällen eine Verarbeitung personenbezogener sensibler Daten zulässig ist. Liegen diese Voraussetzungen – wie im Kontext von Art. 10 Abs. 5 KI-VO-KOM der Fall

[33] *BVMed-Positionen zum Entwurf des „Artificial Intelligence Act"* (AIA), MPR 2021, 176, 178.

– vor, muss die Vorschrift als eigenständige Rechtsgrundlage verstanden werden.[34]

IV. Ausweitung des Anwendungsbereichs des Art. 10 Abs. 5 KI-VO-KOM

Nicht überzeugend ist aber, warum eine solche Regelung nur für Hochrisiko-Systeme gelten soll.[35] Sollte der Ansatz, ein möglich benachteiligungsfreies Ergebnis zu erzielen, nicht für alle KI-Systeme gelten? Es überzeugt nicht, dass sensible Daten nur dann verarbeitet werden, wenn das KI-System größere Risiken für die Grundrechte und Grundfreiheiten der betroffenen Person herbeiführen kann. Zwar gibt es KI-Systeme, die grundsätzlich mit einem niedrigeren Risiko für die Grundrechte und Grundfreiheiten der betroffenen Personen einhergehen. Aber auch bei einem niedrigeren Risiko für die Grundrechte und Grundfreiheiten der betroffenen Person sollten sensible Daten verarbeitet werden, damit Verzerrungen korrigiert werden. Schließlich muss es das Ziel sein, dass ein möglichst benachteiligungsfreies Ergebnis erzeugt wird. Außerdem kann das Risiko einer KI-Anwendung je nach Anwendungsfall unterschiedlich ausfallen. Chatbots fallen beispielsweise nach dem KI-VO-KOM (nicht aber zwingend nach dem KI-VO-PARL) unter KI-Systeme, die ein geringes Risiko aufweisen.[36] Auch Chatbots können aber Risiken für bestimmte Personengruppen aufweisen, etwa wenn Sprachassistenten bestimmte Dialekte oder Akzente nicht gelernt haben und deshalb nicht verstehen.[37] Ebenso können die Antworten von Chatbots diskriminierende Inhalte enthalten. Der Chatbot „*Tay*“ von

---

[34] *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 103, die Art. 10 Abs. 5 KI-VO-KOM als „gesetzliche Verarbeitungsbefugnis“ einordnen.; *Spindler*, in: Hilgendorf/Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur künstlichen Intelligenz, 2023, S. 103 Rn. 31.

[35] Im Ergebnis so auch: *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 62.

[36] Neue Vorschriften für künstliche Intelligenz – Fragen und Antworten, https://perma.cc/U9XC-ZRQM (archiviert am 14.11.2022).

[37] *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen (2020), S. 73.

Microsoft wurde etwa keine 24 Stunden nach seiner Veröffentlichung im Netz wieder abgeschaltet, weil er rassistische und beleidigende Tweets verfasste.[38]

V. Zwischenergebnis: Keine Überschneidung mit Art. 9 DSGVO

1. Art. 10 Abs. 5 KI-VO-KOM verfolgt ein wichtiges Ziel: Angesichts möglicher Verzerrungen durch Hochrisiko-KI-Systeme muss es möglich sein, ggf. auch sensible Daten nach Art. 9 Abs. 1 DSGVO zu verarbeiten.[39] Die Vorschrift erfüllt die Voraussetzungen des Art. 9 Abs. 2 lit. g DSGVO und ist somit als eigenständige Rechtsgrundlage für die Verarbeitung sensibler Daten in bestimmten Fällen einzuordnen.

2. Der Anwendungsbereich des Art. 10 Abs. 5 KI-VO-KOM bezieht sich auf *biases* (Verzerrungen).[40] Unter *bias* i. S. d. Art. 10 Abs. 5 KI-VO-KOM sollte grundsätzlich eine diskriminierende oder sonst benachteiligende Entscheidung gegenüber einer Person durch ein KI-System verstanden werden. Man sollte sich an den Fallgruppen des AGG orientieren, die aber nicht abschließend verstanden werden sollten. Mögliche Verzerrungen in KI-Systemen sollten nicht nur dann erfasst werden, wenn sie im AGG genannt sind. Es können dabei alle Formen von *technical bias*, *pre-existing bias* und *emergent bias* erfasst sein. Diese Kategorien können helfen, die unterschiedlichen *biases* einzuordnen. Anders als im KI-VO-PARL angedeutet, sollten auch gerechtfertigte Benachteiligungen als bias eingestuft werden. Das liegt daran, dass es im Rahmen von Art. 10 Abs. 5 KI-VO-KOM darum geht, dass zunächst alle Formen von *biases* erkannt werden sollen, um diese aufgrund der Verarbeitung zusätzlicher sensibler Daten zu verhindern oder jedenfalls zu verringern. Die Frage, ob eine Verzerrung ggf. gerechtfertigt ist, ist eine nachgelagerte Frage, die im Rahmen von Art. 10 Abs. 5 KI-VO-KOM nicht relevant ist.

3. Der Anwendungsbereich des Art. 10 Abs. 5 KI-VO-KOM sollte sich nicht nur auf Hochrisiko-KI-Systeme beschränken, weil auch bei

---

[38] S. https://perma.cc/88T4-6LWZ (archiviert am 02.07.2023).
[39] Kapitel 11 B.II. (S. 375).
[40] Kapitel 11 B.I. (S. 372).

anderen KI-Systemen Verzerrungen hervorgerufen werden können, die ggf. mithilfe der Verarbeitung sensibler Daten korrigiert werden können.

C. Hohe Datenqualität vs. Grundsatz der Datenminimierung

Die Trainingsdaten müssen gem. Art. 10 Abs. 3 KI-VO-KOM relevant, repräsentativ, fehlerfrei und vollständig sein.[41] Wie bereits herausgearbeitet unterscheidet sich Art. 10 Abs. 3 KI-VO-PARL von den Vorgaben des Art. 10 Abs. 3 KI-VO-KOM. Nach Art. 10 Abs. 3 KI-VO-PARL müssen die Trainingsdaten relevant, hinreichend repräsentativ, angemessen auf Fehler überprüft und im Hinblick auf den beabsichtigten Zweck so vollständig wie möglich sein.

Mit dem Training von Hochrisiko-KI-System geht einher, große Datenbestände zu verarbeiten. Die Ergebnisse algorithmischer Systeme werden aussagekräftiger, wenn möglichst viele qualitativ hochwertige Trainingsdaten verwendet werden.[42] Mit den Vorgaben des zukünftigen Art. 10 Abs. 3 einer KI-VO ist es vereinbar, auch ggf. große Datensätze zum Training zu verwenden. Allerdings steht im Widerspruch zur Verarbeitung großer Datenmengen womöglich der Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO. Nach diesem Grundsatz müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Daten sind dann auf das notwendige Maß beschränkt, wenn der Verarbeitungszweck auch ohne zusätzlich verarbeitete Daten erreicht werden kann.[43] Der Grundsatz der Datenminimierung ist daher nicht so zu verstehen,

---

[41] Kapitel 10 B.I. (S. 345).

[42] *Sun/Li/Liu u.a.*, in: McIntosh/Nguyen (Hrsg.), 2022 ACM/IEEE 44th International Conference on Software Engineering, 2022, S. 1609; *Apel/Kaulartz*, RDi 2020, 24, 26; *Jüngling*, MMR 2020, 440, 441.

[43] Kühling/Buchner/*Herbst*, Art. 5 DSGVO Rn. 57.

dass insgesamt *möglichst wenig* Daten verarbeitet werden.[44] Vielmehr muss man den Grundsatz der Datenminimierung so verstehen, dass nur so viele Daten für das Training von algorithmischen Systemen verwendet werden, wie notwendig sind, um den Zweck zu erreichen. Das ist aber aus zwei Gründen problematisch. Zum einen ist es kaum möglich, von vorneherein abzuschätzen, wie viele Daten man tatsächlich benötigt, um den Zweck – etwa ein System zur Bewerberinnenauswahl zu trainieren – zu erreichen. Zum anderen steht mit dem Grundsatz der Datenminimierung der Prozess des Trainings im Vordergrund. Für das Training muss die Anzahl der personenbezogenen Daten auf das notwendige Maß beschränkt sein. Überzeugender ist es allerdings, das Trainings*ergebnis* in den Vordergrund zu stellen. Je weniger ein System diskriminiert oder sonstige Benachteiligungen hervorruft, desto besser. Das erfordert aber auch, ggf. mehr personenbezogene Daten zu verarbeiten, als für den konkreten Zweck notwendig sind.

Letztlich kann man das Ziel für die Notwendigkeit der Verarbeitung selbst definieren. Solange man begründen kann, warum die Verarbeitung der entsprechenden personenbezogenen Daten notwendig war, um den Zweck zu erreichen, steht die Verarbeitung nicht im Widerspruch zu Art. 5 Abs. 1 lit. c DSGVO. Faktisch kann man eine solche Auslegung dann auch als Umgehung des Art. 5 Abs. 1 lit. c DSGVO einordnen. Eine solche Auslegung ist aber sinnvoll, da Datenminimierung als Grundsatz und ein „gutes" algorithmisches System, welches keine diskriminierenden oder sonst benachteiligenden Ergebnisse hervorruft, sich widersprechen. Außerdem sollte man den Grundsatz der Datenminimierung so verstehen, dass – soweit es möglich ist – keine personenbezogenen, sondern anonymisierte oder synthetische Daten verwendet werden.

---

[44] Kühling/Buchner/*ders.*, Art. 5 DSGVO Rn. 56; *Götz*, Big Data im Personalmanagement, 2020, S. 86 f.; *Meinecke*, Datenschutz und Data Science, 2021, S. 126 ff.; a. A.: *Waas*, Künstliche Intelligenz und Arbeitsrecht, 2022, S. 154; *Steege/Kuß*, in: Kuß/Steege/Chibanguza (Hrsg.), Künstliche Intelligenz, 2022, 1. Teil § 2 C. Rn. 63 m. w. N.

D. Menschliche Überwachung von Hochrisiko-KI-Systemen

Anbieterinnen müssen sicherstellen, dass Hochrisiko-KI-Systeme die Anforderungen in Kapitel 2 des KI-VO-KOM erfüllen. Dazu gehört auch, dass die Systeme so konzipiert sind, dass sie während der Dauer ihrer Verwendung von natürlichen Personen beaufsichtigt werden können (Art. 14 Abs. 1 KI-VO-KOM). Dabei soll die natürliche Person ggf. den Betrieb des Systems stoppen, vgl. Art. 14 Abs. 4 lit. e KI-VO-KOM.

I. Kritik an Art. 14 Abs. 1 KI-VO-KOM

Art. 14 Abs. 1 KI-VO-KOM ist aus zwei Gründen keine gelungene Norm. Zum einen knüpft die Regelung des Art. 14 KI-VO-KOM nicht wie Art. 22 DSGVO daran an, ob das KI-System dazu führt, dass die betroffene Person einer *ausschließlich* automatisierten Entscheidung unterworfen wird, die rechtliche Wirkungen oder ähnliche erhebliche Beeinträchtigungen für sie hat. Solche Entscheidungen sind nach Art. 22 DSGVO verboten.[45] Wenn die finale Entscheidung ohnehin durch einen Menschen getroffen wird und nur vorbereitende Entscheidungen durch das System getroffen werden, ist es wenig überzeugend, warum im laufenden Prozess in das System eingegriffen werden soll.[46] Schließlich liegen die Gefahren letztlich darin, dass der Mensch nach der Verarbeitung durch das System eine hinreichend eigene Entscheidung trifft.[47]

Zum anderen wird die Norm ohnehin praktisch kaum umsetzbar sein. Selbst wenn man den Anwendungsbereich des Art. 14 KI-VO-KOM auf Entscheidungen begrenzt, die auf einer ausschließlich automatisierten Verarbeitung beruhen, ist zu fragen, welche Person fachlich dafür geeignet ist, entsprechend Art. 14 KI-VO-KOM die Aufsicht zu führen.[48] Es wird für eine Person nahezu unmöglich sein, etwaige Anzeichen von Anomalien oder Dysfunktionen zu erkennen (Art. 14 Abs. 4 lit. a KI-VO-KOM).[49] Dem

---

[45] Kapitel 6 D. (S. 204).

[46] *Bomhard/Merkle*, RDi 2021, 276, 281.

[47] Kapitel 6 D.IV.3. (S. 214).

[48] Vgl. *Bomhard/Merkle*, RDi 2021, 276, 281.

[49] Vgl. *Ebers/Hoch/Rosenkranz u.a.*, RDi 2021, 528, 534; *Linardatos*, GPR 2022, 58, 66; kritisch dazu auch: *Geminn*, ZD 2021, 354, 357.

schließen sich auch Stimmen in der Literatur an: Sie halten die Anforderungen des Art. 14 KI-VO-KOM für unrealistisch und sehen die Gefahr, dass die mangelnde Umsetzung von Art. 14 KI-VO-KOM faktisch zu einem Verbot von Hochrisiko-KI-Systemen führen könnte.[50]

Am Ende bleibt die Frage nach der Überwachung des Hochrisiko-KI-Systems eine technische Frage. Wichtiger noch als die mögliche Überwachung eines solchen Systems ist aber die Transparenz. Eine ständige Überwachung ist bei komplexen Verarbeitungsprozessen unrealistisch und mit der Arbeitsweise von KI-Systemen nicht in Einklang zu bringen.

II. Art. 14 KI-VO-PARL als praxistauglichere Vorschrift?

Art. 14 KI-VO-PARL ergänzt die Vorgaben des Art. 14 KI-VO-KOM. Art. 14 Abs. 1 KI-VO-PARL nimmt auf Art. 4b KI-VO-PARL Bezug, in dem Vorgaben für KI-Kenntnisse geregelt sind. Natürliche Personen, die für die menschliche Aufsicht des KI-Systems zuständig sind, müssen ausreichende KI-Kenntnisse haben. Gem. Art. 14 Abs. 2 KI-VO-PARL soll die menschliche Aufsicht insbesondere dann zum Ziel haben, die Risiken für Gesundheit, Sicherheit, Grundrechte oder Umwelt zu vermeiden oder zu minimieren, wenn die menschliche Entscheidung auf ausschließlich automatisierten Entscheidungen beruht und rechtliche oder andere erhebliche Auswirkungen auf die Personen oder Gruppe hat, für die das System angewendet wird. Damit berücksichtigt der KI-VO-PARL zumindest teilweise die oben im Vergleich mit Art. 22 DSGVO geäußerte Kritik an Art. 14 KI-VO-KOM. Nach wie vor soll die Norm aber bei jeglichen Hochrisiko-KI-Systemen anwendbar sein. Konsequenter wäre indes eine Beschränkung der Überwachungspflicht auf Fälle mit ausschließlich automatisierten Entscheidungen gewesen. Faktisch sind solche Entscheidungen im Falle personenbezogener Daten indes ohnehin in weiten Teilen ausgeschlossen, da Art. 22 DSGVO diese verbietet.[51]

Schließlich sieht Art. 14 Abs. 4 lit. e KI-VO-PARL vor, dass ein Hochrisiko-KI-System nicht durch eine „Stop"-Taste oder ein ähnliches Verfahren unterbrochen werden muss, wenn der menschliche Eingriff die Risiken erhöht

---

[50] *Ebers/Hoch/Rosenkranz u.a.*, RDi 2021, 528, 534; *Heil*, MPR 2022, 1, 9.

[51] Kapitel 6 D.V.1. (S. 234).

oder er sich negativ auf die Leistung des Systems auswirken würde. Eine solche Ausnahme ist zu begrüßen. Das Grundproblem aber besteht darin, dass es regelmäßig grundsätzlich schwierig bleibt, die untersuchten KI-Systeme in ihren Prozessen zu unterbrechen.[52]

E. Art. 54 KI-VO-KOM vs. Art. 6 Abs. 4 DSGVO

Art. 53 Abs. 1 KI-VO-KOM sieht vor, dass KI-Reallabore (sog. *regulatory sandboxes*) eingeführt werden, in denen in kontrollierter Umgebung KI-Systeme entwickelt, erprobt und validiert werden können. Nach Art. 54 Abs. 1 KI-VO-KOM dürfen personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme unter bestimmten Bedingungen verarbeitet werden.[53] Art. 54 KI-VO-KOM ist somit eine Ausnahme vom Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO.[54] Nach diesem dürfen personenbezogene Daten grundsätzlich nur zu einem vorher festgelegten Zweck verarbeitet werden.

Die Weiterverarbeitung zu anderen als den ursprünglich festgelegten Zwecken ist in Art. 6 Abs. 4 DSGVO geregelt. Nach dieser Vorschrift kommt eine Weiterverarbeitung zu einem anderen als dem ursprünglichen Zweck auch in Betracht, wenn die Verarbeitung durch eine Rechtsvorschrift der Union oder der Mitgliedstaaten legitimiert wird. Als solche Vorschrift ist Art. 54 Abs. 1 KI-VO-KOM einzuordnen.[55] Zwar soll der KI-VO-KOM – wie auch schon im Rahmen von Art. 10 Abs. 5 KI-VO-KOM – grundsätzlich nicht so verstanden werden, dass er Rechtsgrundlagen für die Verarbeitung

---

[52] Näher dazu s. *Biewer/Baum/Hermanns/Hetmank/Langer/Lauber-Rönsberg/Lehr/Sterz*, Software Doping Analysis for Human Oversight, S. 25, https://perma.cc/7ZJZ-SLR2 (archiviert am 04.11.2023).

[53] Kritisch: *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188, 1192.

[54] *Rostalski/Weiss*, ZfDR 2021, 329, 336 f.; s. zum Grundsatz der Zweckbindung auch: *Härting*, NJW 2015, 3284.

[55] *Hornung*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, S. 91, 104 f.

personenbezogener Daten enthält.[56] Für die KI-Reallabore gilt aber etwas anderes: Im Hinblick auf die personenbezogenen Daten, die für andere Zwecke erhoben werden, soll der KI-VO-KOM nach Erwägungsgrund 72 S. 4 KI-VO-KOM die Rechtsgrundlage zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse innerhalb der KI-Reallabore bilden. Das soll nach dem Wortlaut des Erwägungsgrunds aber „im Einklang" mit Art. 6 Abs. 4 DSGVO, Art. 6 der Verordnung (EU) 2018/1725[57] sowie Art. 4 Abs. 2 JI-Richtlinie[58] erfolgen. Am Wortlaut des Erwägungsgrundes 72 S. 4 KI-VO-KOM ändert sich im KI-VO-PARL nichts, allerdings finden sich diese Erwägungen nicht in Erwägungsgrund 72, sondern in 72a KI-VO-PARL wieder.

Wann genau ein entsprechender „Einklang" mit Art. 6 Abs. 4 DSGVO hergestellt ist, erklärt der Erwägungsgrund nicht. Die Formulierung, dass die Verarbeitung nur möglich ist, wenn sie im Einklang mit etwa Art. 6 Abs. 4 DSGVO erfolgt, deutet darauf hin, dass Art. 6 Abs. 4 DSGVO nach dem KI-VO-PARL nicht als eigenständige Rechtsgrundlage angesehen wird, sondern eine zusätzliche Voraussetzung für die Verarbeitung personenbezogener Daten ist, wenn diese zu anderen als den ursprünglich erhobenen Zwecken verarbeitet werden sollen. Man könnte daher den Erwägungsgrund 72 KI-VO-KOM bzw. Erwägungsgrund 72a KI-VO-PARL so verstehen, dass sowohl die Voraussetzungen des Art. 6 Abs. 4 DSGVO als auch die Voraussetzungen des Art. 54 Abs. 1 einer zukünftigen KI-VO vorliegen müssen, damit die Verarbeitung rechtmäßig ist.

Das überzeugt nicht. Zum einen ist Art. 6 Abs. 4 DSGVO selbst eine eigenständige Rechtsgrundlage.[59] Zum anderen ist ausweislich des KI-VO-KOM als auch des KI-VO-PARL ist Art. 54 Abs. 1 KI-VO-KOM ebenfalls

---

[56] Erwägungsgrund 41 S. 3 KI-VO-KOM; im KI-VO-PARL gestrichen, s. hierzu (Kapitel 11 B.III. S. 376).

[57] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, Abl. L 295 vom 21.11.2018, S. 39.

[58] Abl. L 119 vom 4.5.2016, S. 89.

[59] Kapitel 6 B.IV.1. (S. 133).

eine eigenständige Rechtsgrundlage. Es müssen nicht zwei Rechtsgrundlagen erfüllt sein, um eine Verarbeitung personenbezogener Daten durchzuführen.

Selbst wenn man Art. 6 Abs. 4 DSGVO nicht als eigenständige Rechtsgrundlage einordnet, wäre es reiner Formalismus, neben den strengen Voraussetzungen des Art. 54 Abs. 1 einer zukünftigen KI-VO noch den Kompatibilitätstest[60] nach Art. 6 Abs. 4 DSGVO durchzuführen. Bereits zu Art. 10 Abs. 5 KI-VO-KOM ist Folgendes ausgeführt worden[61]: Es ist kein sinnvoller Regelungsansatz, andere Regulierungen immer unberührt zu lassen. Stattdessen sollten Doppelstrukturen in der Regulierung nach Möglichkeit reduziert werden, damit sie nicht immer komplizierter wird. Die strengen Voraussetzungen des Art. 54 Abs. 1 einer zukünftigen KI-VO genügen, um die Verarbeitung personenbezogener Daten, die ursprünglich für andere Zwecke erhoben wurde, zu rechtfertigen.

F. Betroffenenrechte nach der DSGVO vs. Recht auf Erklärung

Der KI-VO-KOM enthält keine Informationspflichten und gewährt datenschutzrechtlich betroffenen Personen keine Individualrechte. Die Informationspflichten und die Betroffenenrechte der DSGVO[62] gelten aber weiter neben den Regelungen der künftigen KI-VO. Wie bereits herausgearbeitet wurde, ist ein Recht auf Begründung der vom KI-System getroffenen Entscheidung erforderlich, damit die betroffene Person das finale Ergebnis einordnen kann.[63] Ein solches Recht existiert indes auch in der DSGVO (noch) nicht.

Art. 68c KI-VO-PARL sieht hingegen ein solches Recht auf Erklärung der individuellen Entscheidungsfindung vor. Nach dieser Vorschrift hat jede Person, die von einer Entscheidung betroffen ist, welche auf der Grundlage eines Hochrisiko-KI-Systems getroffen wurde und die Rechtsfolgen nach sich zieht oder sie in ähnlicher Weise beeinträchtigt, dass die Entscheidung sich

---

[60] Kapitel 6 B.IV.4. (S. 137).
[61] Kapitel 11 B.III. (S. 376).
[62] Kapitel 7 (S. 241).
[63] Kapitel 7 B.V.3. (S. 259).

nachteilig auf ihre Gesundheit, ihre Sicherheit, ihre Grundrechte, ihr sozioökonomisches Wohlergehen oder auf andere Rechte auswirkt, das Recht auf Erklärung der individuellen Entscheidungsfindung. Dieses Recht umfasst es, von der Bereitstellerin eine klare und aussagekräftige Erklärung gem. Art. 13 Abs. 1 KI-VO-PARL (Transparenzvorgaben) über die Rolle des KI-Systems im Entscheidungsverfahren, über die wichtigsten Parameter der getroffenen Entscheidung und die damit verbundenen Eingabedaten zu erhalten.

Art. 68c Abs. 2 KI-VO-PARL schränkt das Recht auf Erklärung indes ein: Art. 68c Abs. 1 KI-VO-PARL soll nicht für den Einsatz von KI-Systemen gelten, für die im Unionsrecht oder im nationalen Recht Ausnahmen oder Beschränkungen von der Verpflichtung nach Art. 68c Abs. 1 KI-VO-PARL vorgesehen sind. Das soll allerdings nur gelten, sofern diese Ausnahmen oder Beschränkungen den Wesensgehalt der Grundrechte und -freiheiten achten und eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen. Solche Ausnahmen sind bislang noch nicht vorgesehen, weshalb auf die Ausnahmen nach Art. 68c Abs. 2 KI-VO-PARL nicht weiter eingegangen wird.

Art. 68 Abs. 3 KI-VO-PARL stellt klar, dass Art. 68c KI-VO-PARL unbeschadet der Artikel 13, 14, 15 und 22 DSGVO gilt und mithin die Vorgaben der DSGVO ergänzt.

Wie bereits herausgearbeitet wurde, ist ein Recht auf Erklärung der Entscheidung oder auch Recht auf Begründung der Entscheidung notwendig, um mehr Transparenz für die betroffene Person herzustellen.[64] Die in diesem Kontext angesprochenen Erwägungen, dass sich eine Begründungspflicht nur in grundrechtssensiblen Bereichen rechtfertigen lässt, werden mit Art. 68c Abs. 1 KI-VO-PARL umgesetzt. Zwar schützt die in Art. 2 Abs. 1 GG geregelte allgemeine Handlungsfreiheit und die in Art. 16 GrCH geregelte unternehmerische Freiheit auch das Recht der Bereitstellerin, unter Einsatz des KI-Systems Entscheidungen nach eigenem Ermessen zu treffen.[65] Art. 68c

---

[64] Kapitel 7 B.V.3. (S. 259).

[65] BeckOK GG/*Lang*, Art. 2 GG Rn. 9; vgl. Calliess/Ruffert/*Ruffert*, Art. 16 GRCh Rn. 2.

Abs. 1 KI-VO-PARL sieht ein Recht auf Erklärung aber nur dann vor, wenn es sich um Entscheidungen handelt, die auf der Grundlage eines Hochrisiko-KI-Systems getroffen wurden. Das sind Entscheidungen, die Bereiche betreffen, die für die betroffenen Personen grundrechtssensibel sind. In solchen Fällen ist eine Einschränkung der allgemeinen Handlungsfreiheit bzw. der unternehmerischen Handlungsfreiheit verhältnismäßig.[66]

Ebenfalls bereits ausgeführt wurde der Gedanke, dass ein Recht auf Erklärung auch mit technischen Hürden verbunden ist. Es ist häufig technisch schwierig möglich, den Entscheidungsprozess des Systems offenzulegen. Mithilfe von XAI ist es aber – jedenfalls in Teilen – bereits heutzutage möglich, bestimmte Entscheidungsprozesse offenzulegen.[67] Art. 68c Abs. 1 KI-VO-PARL sieht keine Ausnahmen des Rechts auf Erklärung vor, wenn es technisch schwierig oder unmöglich ist, den entsprechenden *Input*, die wichtigsten Parameter und die Bedeutung des KI-Systems im Entscheidungsverfahren offenzulegen. Das ist eine entscheidende Wertung des KI-VO-PARL: Es muss technisch möglich gemacht werden, die Entscheidungen, die mithilfe eines Hochrisiko-KI-Systems getroffen werden, hinreichend zu erklären. Ansonsten – diese eindeutige Aussage ist bislang noch nicht im KI-VO-PARL enthalten – dürfen solche Systeme nicht eingesetzt werden.

Das überzeugt. Zwar ist ein Recht auf Erklärung der individuellen Entscheidung potentiell hinderlich für Hochrisiko-KI-Systeme. Ein solches Recht ist aber notwendig, um einen grundrechtskonformen Einsatz sicherzustellen. Um die Grundrechte und Grundfreiheiten der betroffenen Personen zu gewährleisten, muss es im Einzelfall möglich sein, die individuelle Entscheidung erklären zu können. Im Übrigen trägt ein solches Recht dazu bei, dass das Vertrauen der betroffenen Person in das betreffende System gestärkt wird.

---

[66] Vgl. Kapitel 7 B.V.3 (S. 259).

[67] Kapitel 4 A.II (S. 42).

G. Zwischenergebnis: Vorschriften des KI-VO-KOM berücksichtigen die DSGVO nicht hinreichend

1. Die Ausführungen zeigen: Die Vorschriften des KI-VO-KOM berücksichtigen nicht hinreichend das Verhältnis zur DSGVO. Um eine sinnvolle Ergänzung zur DSGVO zu bilden, sollte die zukünftige KI-VO in manchen Punkten nachgebessert werden. Der KI-VO-PARL enthält – wie bereits ausgeführt – gegenüber dem KI-VO-KOM bereits einige Verbesserungen.

2. Die Pflicht, eine DSFA durchzuführen und die Pflicht, ein Risikomanagementsystem nach Art. 9 Abs. 1 einer zukünftigen KI-VO einzurichten und aufrechtzuerhalten, betreffen unterschiedliche Personen. [68] Bei anderen Risikobewertungen können jedoch Synergieeffekte zwischen den in der DSFA angestellten Erwägungen und den weiteren Risikobewertungen genutzt werden: Richtigerweise verweist Art. 29a Abs. 6 und Art. 54 Abs. 1 c KI-VO-PARL daher auf Art. 35 DSGVO. [69] Insbesondere im Rahmen von Art. 29a KI-VO-PARL ist es überzeugend, dass die Erwägungen, die in der DSFA eine Rolle spielen, erneut aufgegriffen werden. Die Pflicht, eine DSFA gem. Art. 35 DSGVO durchzuführen sowie eine grundrechtliche Folgeabschätzung vorzunehmen, trifft zumeist dieselbe Person, nämlich die Arbeitgeberin.

3. Mit Inkrafttreten der KI-VO soll sich nach dem KI-VO-KOM nichts daran ändern, dass die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in der DSGVO geregelt sind. Obwohl Art. 10 Abs. 5 KI-VO-KOM eine Ausnahme von Art. 9 Abs. 2 lit. g DSGVO vorsieht und damit eigentlich als eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten einzustufen ist, soll Art. 10 Abs. 5 KI-VO-KOM nicht als solche gelten. Dieses bislang in Erwägungsgrund 41 KI-VO-KOM genannte Verständnis von Art. 10 Abs. 5 KI-VO-KOM wird in Erwägungsgrund

---

[68] Kapitel 11 A.I. (S. 363).

[69] Kapitel 11 A.II. (S. 368); Kapitel 11 A.III (S. 370).

41 KI-VO-PARL richtigerweise nicht mehr erwähnt. Vielmehr führt Art. 10 Abs. 5 KI-VO-PARL nun weitere Voraussetzungen auf, unter denen eine Verarbeitung besonderer Kategorien personenbezogener Daten möglich ist. Liegen diese Voraussetzungen vor, müssen keine zusätzlichen Voraussetzungen nach der DSGVO erfüllt sein.[70] Bei einer finalen Regelung des Art. 10 Abs. 5 KI-VO sollten, anders als im KI-VO-PARL angedeutet, auch gerechtfertigte Benachteiligungen als bias eingestuft werden. Das liegt daran, dass es im Rahmen von Art. 10 Abs. 5 KI-VO-KOM darum geht, dass zunächst alle Formen von *biases* erkannt werden sollen, um diese aufgrund der Verarbeitung zusätzlicher sensibler Daten zu verhindern oder jedenfalls zu verringern. [71] Der Anwendungsbereich eines zukünftigen Art. 10 Abs. 5 KI-VO sollte sich nicht nur auf Hochrisiko-KI-Systeme beschränken, weil auch bei anderen KI-Systemen Verzerrungen hervorgerufen werden können, die ggf. mithilfe der Verarbeitung sensibler Daten korrigiert werden können.[72]

4. Art. 54 Abs. 1 KI-VO-KOM und Art. 54 Abs. 1 KI-VO-PARL statuieren eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, die ursprünglich für andere Zwecke erhoben wurden. Die Verarbeitung ist ausschließlich zum Zweck der Entwicklung und Prüfung bestimmter innovativer KI-Systeme in der „*regulatory sandbox*" unter bestimmten, in Art. 54 KI-VO-KOM oder KI-VO-PARL genannten Bedingungen möglich. Das Verhältnis zur DSGVO ist aber auch nach Art. 54 KI-VO-PARL nicht hinreichend geregelt. Es überzeugt nicht, dass neben den Voraussetzungen des Art. 54 KI-VO-PARL die Verarbeitung in Einklang mit Art. 6 Abs. 4 DSGVO erfolgen muss. [73] Die Formulierung „in Einklang mit den Vorgaben des Art. 6 Abs. 4 KI-VO" deutet aber darauf hin, dass die Voraussetzungen des Art. 6 Abs. 4 KI-VO neben den Voraussetzungen des Art. 54 Abs. 1 KI-VO-PARL ebenfalls vorliegen müssen. Von diesem Erfordernis sollte die zukünftige KI-VO absehen. Wenn die

[70] Kapitel 11 B.III. (S. 376).
[71] Kapitel 11 B.I. (S. 372).
[72] Kapitel 11 B.IV. (S. 378).
[73] Kapitel 11 E. (S. 384).

strengen Voraussetzungen des Art. 54 Abs. 1 KI-VO-PARL erfüllt sind, müssen nicht auch noch die Voraussetzungen des Art. 6 Abs. 4 DSGVO vorliegen. Andernfalls hat Art. 54 Abs. 1 KI-VO-PARL keinen echten Mehrwert.

5. Schließlich geht der KI-VO-KOM über die Anforderungen der DSGVO hinaus. Art. 22 DSGVO knüpft an eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung an, Art. 14 KI-VO-KOM sieht hingegen eine Überwachung von Hochrisiko-KI-Systemen durch einen Menschen vor, unabhängig von der „Ausschließlichkeit" der automatisierten Entscheidung. Wie bei Art. 14 KI-VO-KOM deutlich wird, wird die Norm in praktischer Hinsicht zu womöglich unüberwindbaren Schwierigkeiten führen. Welche Person wird in der Lage sein, im laufenden Prozess eines Systems bei Anomalien o. Ä. einzugreifen und den Verarbeitungsprozess zu stoppen? An dieser Stelle bessert der KI-VO-PARL nach.[74] Die Person, die das Hochrisiko-KI-System überwachen soll, muss entsprechende KI-Kenntnisse aufweisen (Art. 14 Abs. 1 KI-VO-PARL). Das bedeutet, dass unter anderem grundlegende Kenntnisse und Fähigkeiten in Bezug auf KI-Systeme und ihre Funktionsweise, einschließlich der verschiedenen Arten von Produkten und Verwendungen sowie ihrer Risiken und Vorteile vermittelt werden (Art. 4b Abs. 3 KI-VO-PARL). Es wird aber gleichwohl schwierig sein, die untersuchten KI-Systeme in ihrem Prozess zu unterbrechen.

6. Schwierigkeiten bereiten die Vorgaben des KI-VO-KOM an die Trainingsdatenqualität [75] im Hinblick auf den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO.[76] Allerdings steht die Verarbeitung personenbezogener Daten nicht im Widerspruch zu Art. 5 Abs. 1 lit. c DSGVO, wenn man begründen kann, warum die Verarbeitung der entsprechenden personenbezogenen Daten notwendig war, um den Zweck zu erreichen. Faktisch kann man eine

---

[74] Kapitel 11 D.II. (S. 383).
[75] Kapitel 10 B.I. (S. 345).
[76] Kapitel 11 C. (S. 380).

solche Auslegung dann auch als Umgehung des Art. 5 Abs. 1 lit. c DSGVO einordnen, weil man selbst definieren kann, was „notwendig" war. Eine solche Auslegung ist aber sinnvoll, da Datenminimierung an sich und ein „gutes" algorithmisches System, welches keine diskriminierenden oder sonst benachteiligenden Ergebnisse hervorruft, sich widersprechen. Außerdem sollte man den Grundsatz der Datenminimierung so verstehen, dass – soweit es möglich ist – keine personenbezogenen, sondern anonymisierte oder synthetische Daten verwendet werden.

7. Schließlich enthält der KI-VO-KOM keine Betroffenenrechte. Art. 68c Abs. 1 KI-VO-PARL normiert hingegen ein Recht auf Erklärung der individuellen Entscheidung. Ein solches Recht ist notwendig.[77] Von diesem Recht werden keine Ausnahmen gemacht, wenn es technisch schwierig oder unmöglich ist, den entsprechenden *Input*, die wichtigsten Parameter und die Bedeutung des KI-Systems im Entscheidungsverfahren offenzulegen. Das ist eine entscheidende Wertung des KI-VO-PARL: Es muss technisch möglich gemacht werden, die Entscheidungen, die mithilfe eines Hochrisiko-KI-Systems getroffen werden, hinreichend zu erklären. Ansonsten – diese eindeutige Aussage ist bislang noch nicht im KI-VO-PARL enthalten – dürfen solche Systeme nicht eingesetzt werden. Art. 68 Abs. 3 KI-VO-PARL regelt zudem, dass Art. 68c KI-VO-PARL unbeschadet der Artikel 13, 14, 15 und 22 DSGVO gilt und ergänzt mithin die Vorgaben der DSGVO.

---

[77] Kapitel 7 B.V.3. (S. 259).

Teil 4

Zusammenfassung

1. Der KI-VO-KOM richtet sich gem. Art. 2 Abs. 1 KI-VO-KOM an Anbieterinnen und Nutzerinnen, [1] wobei die meisten Pflichten Anbieterinnen treffen. Die Entwicklerin des KI-Systems ist typischerweise eine Anbieterin i. S. d. KI-VO-KOM, weil sie ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen. Die Arbeitgeberin, die das KI-System im eigenen Unternehmen einsetzt, ist hingegen keine Anbieterin, sondern regelmäßig die Nutzerin gem. Art. 2 Nr. 4 KI-VO-KOM, weil sie das KI-System nicht modifizieren und als eigenes System vermarkten möchte.

2. Der Begriff der Nutzerin wird im KI-VO-PARL sinnvollerweise in den Begriff Bereitstellerin geändert. So kommt es nicht zu Verwechselungen, wenn man diejenigen Personen bezeichnen möchte, die ein KI-System als Endnutzerinnen direkt verwenden. Die finale KI-VO sollte für alle drei Akteurinnen – Anbieterinnen, Bereitstellerinnen und Nutzerinnen – eine Definition bereithalten, damit man zwischen den drei Begriffen eindeutig abgrenzen kann.

3. Anbieterinnen von Hochrisiko-KI-Systemen müssen die Anforderungen des Kapitel 2 KI-VO-KOM erfüllen.

4. Außerdem müssen die Trainings-, Test- und Validierungsdatensätze den Anforderungen nach Art. 10 Abs. 2 bis 5 KI-VO-KOM genügen.[2] Gem. Art. 10 Abs. 3 KI-VO-KOM müssen die Trainingsdaten *relevant,*

---

[1] Kapitel 5 A.IV.3.b) (S. 79); Kapitel 10 A. (S. 341).

[2] Kapitel 10 B.I. (S. 345).

repräsentativ, fehlerfrei und *vollständig* sein. Nach dem Wortlaut des Art. 10 Abs. 3 KI-VO-PARL ändert sich an den vier Merkmalen nichts; allerdings sind diese gemäß Art. 10 Abs. 3 KI-VO-PARL – anders als im KI-VO-KOM – sinnvollerweise einer Abwägung zugänglich: Die Trainingsdaten müssen relevant, *hinreichend repräsentativ*, *angemessen auf Fehler überprüft* und im Hinblick auf den beabsichtigten Zweck *so vollständig wie möglich* sein.

5. Das Merkmal der *relevanten Datensätze* muss so verstanden werden, dass vermieden werden soll, dass viele Daten zu Trainingszwecken genutzt werden, die an sich nicht für den Trainingszweck geeignet sind.

6. Trainingsdaten sind dann *repräsentativ*, wenn bei den für das Training charakteristischen Datenkategorien keine Benachteiligungen angelegt sind. Als Anhaltspunkt für den Begriff der Benachteiligung sollte man das AGG heranziehen. Die im AGG aufgeführten Benachteiligungen sind allerdings nicht abschließend. Bei pseudonymisierten und anonymisierten Daten muss man ebenfalls darauf achten, dass die Daten repräsentativ sind. Für derartigen Daten gelten keine anderen Anforderungen.

7. Ein Datensatz ist *vollständig,* wenn das algorithmische System alle notwendigen Datenkategorien abbildet, um ein bestimmtes Ergebnis zu präsentieren.

8. Beim Merkmal der *Fehlerfreiheit* bleibt unklar, was genau Fehlerfreiheit bedeutet. Ob ein Datum keinen „Fehler“ wie etwa Mess- und Festplattenfehler aufweist und ob es sachlich richtig ist, ist nicht anhand eines konkreten Einzeldatums feststellbar.

9. Der eigene Regelungszweck der Vorgabe des Art. 10 Abs. 3 S. 2 KI-VO-KOM, nach der die Trainingsdatensätze geeignete statistische Merkmale aufweisen müssen, ist fraglich. Einen Unterschied zum Merkmal der Repräsentativität kann man darin sehen, dass bei Art. 10 Abs. 3 S. 2 KI-VO-KOM der konkrete Einsatzbereich des Hochrisiko-KI-Systems im

Fokus steht, wohingegen es beim Merkmal der Repräsentativität darauf nicht vorrangig ankommt.

10. Art. 13 Abs. 1 KI-VO-KOM regelt, dass Anbieterinnen ihre Hochrisiko-KI-Systeme in einer Weise konzipieren und entwickeln müssen, dass sie transparent betrieben werden, damit die Nutzerinnen die Ergebnisse des Systems angemessen interpretieren und verwenden können. Dabei sollten die inhaltlichen Maßstäbe der Informationspflicht nach Art. 13 Abs. 2 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO gelten[3], weil der verfolgte Zweck identisch ist.

11. Sinnvoll ist es, dass Art. 13 Abs. 1 KI-VO-PARL den Anwendungsbereich auf Anbieterinnen ausweitet.

12. Die Anforderungen an Hochrisiko-KI-Systeme sind als „Muss-Vorschriften" ausgestaltet. Werden die Anforderungen nicht erfüllt, werden Geldbußen verhängt.

13. Die Vorschriften des KI-VO-KOM berücksichtigen nicht hinreichend das Verhältnis zur DSGVO.[4] Um eine sinnvolle Ergänzung zur DSGVO zu bilden, sollte die zukünftige KI-VO in manchen Punkten nachgebessert werden. Der KI-VO-PARL enthält – wie bereits ausgeführt – gegenüber dem KI-VO-KOM bereits einige Verbesserungen.

14. Zwar ist es überzeugend, dass die Pflicht, eine DSFA durchzuführen und die Pflicht, ein Risikomanagementsystem nach Art. 9 Abs. 1 einer zukünftigen KI-VO einzurichten und aufrechtzuerhalten, unterschiedliche Personen betreffen.[5] Bei anderen Risikobewertungen können jedoch Synergieeffekte zwischen den in der DSFA angestellten Erwägungen und den weiteren Risikobewertungen genutzt werden.[6]

---

[3] Kapitel 7 B.III.1. (S. 267).
[4] S. Kapitel 11 B. (S. 371).
[5] Kapitel 11 A.I. (S. 363).
[6] Kapitel 11 A.II. (S. 368); Kapitel 11 A.III. (S. 370).

15. Art. 10 Abs. 5 KI-VO-PARL führt nun weitere Voraussetzungen auf, unter denen eine Verarbeitung besonderer Kategorien personenbezogener Daten möglich ist. Liegen diese Voraussetzungen vor, müssen keine zusätzlichen Voraussetzungen nach der DSGVO erfüllt sein.[7] Bei einer finalen Regelung des Art. 10 Abs. 5 KI-VO sollten, anders als im KI-VO-PARL angedeutet, auch gerechtfertigte Benachteiligungen als *biases* eingestuft werden. Das liegt daran, dass es im Rahmen von Art. 10 Abs. 5 KI-VO-KOM darum geht, dass zunächst alle Formen von *biases* erkannt werden sollen, um diese aufgrund der Verarbeitung zusätzlicher sensibler Daten zu verhindern oder jedenfalls zu verringern.[8] Der Anwendungsbereich eines zukünftigen Art. 10 Abs. 5 KI-VO sollte sich nicht nur auf Hochrisiko-KI-Systeme beschränken, weil auch bei anderen KI-Systemen Verzerrungen hervorgerufen werden können.[9]

16. Art. 54 Abs. 1 KI-VO-KOM und Art. 54 Abs. 1 KI-VO-PARL statuieren eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, die ursprünglich für andere Zwecke erhoben wurden. Das Verhältnis zur DSGVO ist aber auch nach Art. 54 KI-VO-PARL nicht hinreichend geregelt. Es überzeugt nicht, dass neben den Voraussetzungen des Art. 54 KI-VO-PARL die Verarbeitung in Einklang mit Art. 6 Abs. 4 DSGVO erfolgen muss.[10] Die Formulierung „in Einklang mit den Vorgaben des Art. 6 Abs. 4 KI-VO" deutet aber darauf hin, dass die Voraussetzungen des Art. 6 Abs. 4 KI-VO neben den Voraussetzungen des Art. 54 Abs. 1 KI-VO-PARL ebenfalls vorliegen müssen. Von diesem Erfordernis sollte die zukünftige KI-VO absehen, damit die Vorschrift einen Mehrwert hat. Wenn die strengen Voraussetzungen des Art. 54 Abs. 1 KI-VO-PARL erfüllt sind, müssen nicht auch noch die Voraussetzungen des Art. 6 Abs. 4 DSGVO vorliegen.

---

[7] Kapitel 11 B.III. (S. 376).
[8] Kapitel 11 B.I. (S. 372).
[9] Kapitel 11 B.IV. (S. 378).
[10] Kapitel 11 E. (S. 384).

17. Gem. Art. 14 KI-VO-KOM müssen Hochrisiko-KI-Systeme durch einen Menschen überwacht werden. Wie bei Art. 14 KI-VO-KOM deutlich wird, wird die Norm in praktischer Hinsicht zu womöglich unüberwindbaren Schwierigkeiten führen. Welche Person wird in der Lage sein, im laufenden Prozess eines Systems bei Anomalien o. Ä. einzugreifen und den Verarbeitungsprozess zu stoppen? An dieser Stelle bessert der KI-VO-PARL nach.[11] Die Person, die das Hochrisiko-KI-System überwachen soll, muss entsprechende KI-Kenntnisse aufweisen (Art. 14 Abs. 1 KI-VO-PARL). Das bedeutet, dass unter anderem grundlegende Kenntnisse und Fähigkeiten in Bezug auf KI-Systeme und ihre Funktionsweise, einschließlich der verschiedenen Arten von Produkten und Verwendungen sowie ihrer Risiken und Vorteile vermittelt werden (Art. 4b Abs. 3 KI-VO-PARL). Es wird aber gleichwohl schwierig sein, die untersuchten KI-Systeme in ihrem Prozess zu unterbrechen.

18. Schwierigkeiten bereiten die Vorgaben des KI-VO-KOM an die Trainingsdatenqualität [12] im Hinblick auf den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO.[13] Allerdings steht die Verarbeitung personenbezogener Daten nicht im Widerspruch zu Art. 5 Abs. 1 lit. c DSGVO, wenn man begründen kann, warum die Verarbeitung der entsprechenden personenbezogenen Daten notwendig war, um den Zweck zu erreichen. Außerdem sollte man den Grundsatz der Datenminimierung so verstehen, dass – soweit es möglich ist – keine personenbezogenen, sondern anonymisierte oder synthetische Daten verwendet werden.

19. Schließlich enthält der KI-VO-KOM keine Betroffenenrechte. Art. 68c Abs. 1 KI-VO-PARL normiert hingegen ein Recht auf Erklärung der individuellen Entscheidung. Ein solches Recht ist notwendig.[14]

---

[11] Kapitel 11 D.II. (S. 383).
[12] Kapitel 10 B.I. (S. 345).
[13] Kapitel 11 C. (S. 380).
[14] Kapitel 7 B.V.3. (S. 259).

Kapitel 12

Zusammenfassung der Ergebnisse

A. Algorithmische Systeme: technischer Hintergrund und Einsatz

1. Algorithmische Systeme sind im Kontext dieser Arbeit Softwaresysteme, die Menschen bewerten und algorithmenbasiert Entscheidungen treffen.[1] Häufig kommen diese Systeme unter Einsatz maschineller Lernmethoden zustande. Solche Systeme werden im Kontext dieser Arbeit als maschinell lernende Systeme oder (Hochrisiko-)KI-Systeme bezeichnet. Maschinelles Lernen beschreibt den Vorgang, dass ein Modell derart programmiert wird, dass es bestimmte Trainingsdaten analysiert und daraus Muster ableitet, sodass ein Algorithmus entsteht, der andere (unbekannte) Daten als die Trainingsdaten verarbeiten kann. Der Lernprozess besteht insbesondere darin, dass die relevanten Parameter des Modells auf Basis der Trainingsdaten und Erfahrungswerte optimiert werden. Es gibt verschiedene Lernstile und Lernverfahren.[2] Algorithmische Systeme müssen aber nicht zwingend mithilfe maschineller Lernmethoden erstellt werden. Es gibt auch Systeme, die ausschließlich nach unmittelbar von Menschen einprogrammierten Regeln im Sinne eines „Wenn-Dann-Schemas“ funktionieren. Auch solche nicht-lernenden Systeme fallen nach dem Verständnis dieser Arbeit unter die Definition eines algorithmischen Systems. Rechtliche Herausforderungen stellen sich aber insbesondere beim Umgang mit maschinell lernenden Systemen, sodass der Fokus der Untersuchung auf solchen Systemen liegt.

---

[1] Kapitel 1 A. (S. 9).

[2] S. dazu näher unter: Kapitel 1 C. (S. 12).

2. Es gibt zahlreiche Anwendungsszenarien algorithmischer Systeme, die bei arbeitsrechtlichen Auswahlentscheidungen vor allem unterstützend eingesetzt werden. [3] Ein großer Anwendungsbereich ist das Bewerbungsverfahren: Neben Systemen, die geeignete Kandidatinnen vorschlagen, können auch Chatbots zur Kommunikation mit den Bewerberinnen eingesetzt werden oder Bewerbungsprozesse per Video- oder Sprachanalyse durchgeführt werden. Hilfreich sind solche Systeme vor allem dann, wenn es darum geht, eine Vielzahl von Bewerbungen auszuwerten. Personalerinnen können aufgrund des Einsatzes algorithmischer Systeme insbesondere beim Vorfiltern der Bewerbungen unterstützt werden.

3. Bei der Vorfilterung einer Vielzahl von Bewerbungen sind algorithmische Systeme menschlichen Entscheidungen in bestimmter Hinsicht überlegen: Sie können große Datenmengen schneller analysieren.[4] Hinzu kommt, dass sie nicht tagesformabhängig sind und anhand feststehender Regeln entscheiden: Algorithmische Systeme lassen sich also nicht von äußeren Umständen beeinflussen und sind daher auf den ersten Blick objektiver als menschliche Entscheidungen. Nicht-lernende Systeme können jedoch nicht flexibel agieren. Das ist zwar bei maschinell lernenden Systemen anders. Es besteht jedoch die Gefahr, dass maschinell lernende Systeme aufgrund bestimmter Korrelationen zwischen Merkmalen zu einem Ergebnis kommen, obwohl keine Kausalität zwischen den Merkmalen besteht. [5] So entstehen auch Benachteiligungsrisiken: Etwa kann es sein, dass ein maschinell lernendes System eine Korrelation zwischen langen Anfahrtswegen von Kandidatinnen und ihrem Kündigungsverhalten analysiert. Lehnt es in der Folge Kandidatinnen mit längeren Anfahrtswegen ab, kann dies zu Benachteiligungen bestimmter Bevölkerungsgruppen führen, die tendenziell eher außerhalb der Stadtmitte wohnen.[6]

---

[3] Kapitel 2 (S. 23).
[4] Kapitel 3 B. (S. 35).
[5] Kapitel 3 C. (S. 36).
[6] Kapitel 8 B.II. (S. 289).

B. Transparenzanforderungen an algorithmische Systeme

4. Die Intransparenz maschinell lernender Systeme ist sowohl auf technischer als auch rechtlicher Ebene ein Problem für das Vertrauen und mithin auch für die Akzeptanz von derartigen Systemen und den von diesen generierten Entscheidungen. Der Transparenzbegriff wird nicht einheitlich verwendet. Transparenz setzt sich nach dem Verständnis dieser Arbeit aus Nachvollziehbarkeit und Erklärbarkeit zusammen. [7] Auf materieller Ebene muss die betroffene Person nachvollziehen können, welche Kriterien die Grundlage für die Entscheidung waren (Nachvollziehbarkeit). Die konkrete Entscheidung muss für die Person verständlich sein. Auf formeller Ebene sollte die betroffene Person die grundsätzliche Funktionsweise des Systems, welches zur Entscheidung geführt hat oder unterstützend zur Entscheidung eingesetzt wurde, verstehen können (Erklärbarkeit).[8]

5. Die maßgeblichen Vorschriften zur Förderung von Transparenz sind Art. 13 Abs. 2 lit. f DSGVO, 14 Abs. 2 lit. g DSGVO sowie 15 Abs. 1 lit. h DSGVO.[9] Nach diesen Vorschriften hat die betroffene Person das Recht, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erhalten. *De lege lata* gelten diese Informationspflichten nach dem Wortlaut der Vorschriften indes nur für ausschließlich automatisierte Entscheidungen, die gem. Art. 22 Abs. 2 DSGVO unter bestimmten Voraussetzungen ausnahmsweise zulässig sind. [10] Gleichwohl sollten bei grundrechtssensiblen Entscheidungen, mithin also auch bei arbeitsrechtlichen Auswahlentscheidungen, die Pflichten *de lege ferenda* nicht länger auf ausschließlich automatisierte Entscheidungen begrenzt sein.[11] Werden algorithmische Systeme entscheidungsunterstützend eingesetzt, kann das Ergebnis des Systems sich erheblich auf die menschliche

---

[7] Kapitel 4 B.I. (S. 45).

[8] Zu diesem zutreffenden Verständnis s. *Knitter*, Digitale Weisungen, 2022, S. 154 f.

[9] Kapitel 7 B. (S. 246).

[10] S. zu den Ausnahmen nach Art. 22 Abs. 2 DSGVO: Kapitel 6 D.IV.5. (S. 224).

[11] Kapitel 7 B.V.1. (S. 257).

Letztentscheidung auswirken.[12] Auch entscheidungsunterstützende Systeme sind für die Grundrechte der betroffenen Person gefährlich, weshalb die betroffene Person über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen der Verarbeitung informiert werden sollte.

6. Die involvierte Logik meint die grundsätzliche Funktionsweise des Algorithmus bzw. Systems sowie die relevanten Parameter.[13] Im Hinblick auf die Tragweite sowie die Auswirkungen der Verarbeitung muss die Person darüber in Kenntnis gesetzt werden, welche möglichen Auswirkungen die Verarbeitung auf ihre Grundrechte hat und welche Schutzmaßnahmen für ihre personenbezogenen Daten ergriffen werden.[14]

7. Die Informationen müssen gem. Art. 12 Abs. 1 S. 1 DSGVO in präziser und transparenter Form dargestellt sowie verständlich und leicht zugänglich präsentiert werden. Sie müssen daher auf den Empfängerhorizont der betroffenen Person zugeschnitten sein und dürfen keine irrelevanten Informationen enthalten.[15] Es ist nicht vorgeschrieben, Bildsymbole zu verwenden. *De lege ferenda* sollte es indes eine Pflicht zur Verwendung von Bildsymbolen oder ggf. auch von Darstellungen per Video geben.[16] Grund dafür ist, dass eine Informationsvermittlung in Textform weniger zugänglich ist und die Gefahr besteht, dass die betroffene Person die Information nicht zur Kenntnis nimmt. Gäbe es eine Pflicht zur Verwendung effektiverer alternativer Informationsmittel, würde sichergestellt werden, dass der tatsächliche Informationseffekt größer wäre.

8. Ein Recht auf Begründung der Entscheidung, die unterstützend mit maschinell lernenden Systemen getroffen wurde, ist nach der DSGVO

---

[12] S. dazu: Kapitel 6 D.IV.3.b) (S. 216).
[13] Kapitel 7 B.III.1.a) (S. 250).
[14] Kapitel 7 B.III.2. (S. 253).
[15] Kapitel 7 B.IV.2. (S. 254).
[16] Kapitel 7 B.V.2. (S. 258).

nicht vorgesehen.[17] Es wäre aber sinnvoll, ein Recht auf Begründung in bestimmten Fällen einzuführen, um mehr Transparenz für die betroffene Person herzustellen. Eine solche Begründungspflicht lässt sich – wie *Martini* zutreffend ausführt – nur in grundrechtssensiblen Bereichen rechtfertigen. Maschinell lernende Systeme haben anders als Menschen kein tiefergehendes Verständnis für die Entscheidung, sie treffen die Entscheidung korrelativ und können ungeahnte „Fehler" machen. [18] Ein Recht auf Begründung ist allerdings sowohl mit rechtlichen als auch mit technischen Hürden verbunden: Zum einen können legitime Interessen Dritter einer Begründung der Entscheidung gegenüberstehen. Hierunter fällt z. B. der Schutz von Geschäftsgeheimnissen. Zum anderen ist es technisch kaum möglich, den Entscheidungsprozess des Systems offenzulegen. Mithilfe von XAI[19] können aber – jedenfalls in Teilen – bereits heutzutage bestimmte Entscheidungsprozesse erklärt werden.

9. In Art. 68c KI-VO-PARL wird erstmals in einem Gesetzesentwurf ein Recht auf Begründung der individuellen Entscheidungsfindung vorgeschlagen.[20] Art. 68c Abs. 1 KI-VO-PARL sieht keine Ausnahmen des Rechts auf Erklärung vor, wenn es technisch schwierig oder unmöglich ist, den entsprechenden *Input*, die wichtigsten Parameter und die Bedeutung des KI-Systems im Entscheidungsverfahren offenzulegen. Das ist eine entscheidende Wertung des KI-VO-PARL, die überzeugt. Es muss technisch möglich gemacht werden, die Entscheidungen, die mithilfe eines Hochrisiko-KI-Systems getroffen werden, hinreichend zu erklären. Ein solches Recht ist notwendig, um einen grundrechtskonformen Einsatz sicherzustellen. Gem. Art. 68 Abs. 3 KI-VO-PARL werden die Informationspflichten nach der DSGVO durch die Vorschrift ergänzt: Art. 68c KI-VO-PARL gilt unbeschadet der Artikel 13, 14, 15 und 22 DSGVO und ergänzt mithin ebenfalls die Vorgaben der DSGVO.

---

[17] Kapitel 7 B.V.3. (S. 259).
[18] S. Kapitel 7 B.V.3. (S. 259).
[19] Kapitel 4 A.II. (S. 42).
[20] Kapitel 11 F. (S. 386).

10. Nach Art. 13 KI-VO-KOM müssen Hochrisiko-KI-Systeme von Anbieterinnen so konzipiert und entwickelt werden, dass ihr Betrieb hinreichend transparent ist, damit die Nutzerinnen die Ergebnisse angemessen interpretieren und verwenden können.[21] Die Vorgaben des Art. 13 Abs. 1 KI-VO-PARL unterscheiden sich inhaltlich nur unwesentlich von Art. 13 Abs. 1 KI-VO-KOM, sodass die Inhalte der Informationspflichten nach Art. 13 Abs. 1 lit. f sowie Art. 14 Abs. 2 lit. g DSGVO herangezogen werden sollten.[22] Trotz der Vorgaben des Art. 13 Abs. 1 KI-VO-KOM oder PARL bleibt es das Wesen eines Hochrisiko-KI-Systems, dass eine Erklärbarkeit nicht einfach umgesetzt werden kann:[23] Auch für die Herstellerinnen des KI-Systems selbst ist es mitunter nicht erklärbar, wie ein Ergebnis zustande gekommen ist.

C. Erfordernis einer Verarbeitungsgrundlage

11. Für algorithmische Systeme, die personenbezogene Daten verarbeiten, ist in aller Regel der Anwendungsbereich der DSGVO in persönlicher (Art. 1 Abs. 1 DSGVO), sachlicher (Art. 2 DSGVO) und räumlicher (Art. 3 DSGVO) Hinsicht eröffnet.[24] Damit die Verarbeitung der personenbezogenen Daten rechtmäßig ist, muss eine Verarbeitungsgrundlage nach Art. 6 DSGVO und ggf. Art. 9 Abs. 2 DSGVO vorliegen.[25] Sollen die personenbezogenen Daten für die Zwecke eines konkreten Beschäftigungsverhältnisses verarbeitet werden, war bislang die Rechtsgrundlage des § 26 Abs. 1 S. 1 BDSG maßgeblich, die auf der Öffnungsklausel des Art. 88 Abs. 1 DSGVO beruht.[26] Diese Norm ist indes seit dem Urteil des EuGH vom 30. März 2023 nicht mehr anwendbar.[27] In der Konsequenz sind auch im Beschäftigungskontext die Rechtsgrundlagen der DSGVO,

---

[21] Kapitel 10 B.II. (S. 355).
[22] Kapitel 7 B.III. (S. 250).
[23] Vgl. Kapitel 1 C.II. (S.17); Kapitel 4 A. (S. 40).
[24] Kapitel 5 A.III.2. (S. 65).
[25] Zum Verhältnis von Art. 6 DSGVO zu Art. 9 DSGVO s. Kapitel 6 A.II.1.b) (S. 105).
[26] Kapitel 5 B.II.1.a) (S. 89).
[27] Kapitel 5 B.II.1.c) (S. 92).

insbesondere Art. 6 Abs. 1 S. 1 lit. b DSGVO, maßgeblich.[28] Wird das Ergebnis des algorithmischen Systems als Grundlage für die Entscheidung herangezogen, muss zudem Art. 22 DSGVO berücksichtigt werden.[29] Aufgrund der unterschiedlichen Anforderungen der jeweiligen Vorschriften wird in dieser Arbeit daher nach drei Verarbeitungsstadien differenziert[30]: Das erste Verarbeitungsstadium befasst sich mit dem Training algorithmischer Systeme.[31] Das zweite Verarbeitungsstadium ist der Einsatz des algorithmischen Systems für ein konkretes Beschäftigungsverhältnis.[32] Das letzte Verarbeitungsstadium ist betroffen, wenn das Ergebnis des Systems als Grundlage für die konkrete Auswahlentscheidung herangezogen wird.[33]

12. Werden algorithmische Systeme trainiert, kann man erwägen, anonymisierte Daten zu verwenden, soweit dies technisch möglich ist. Der Anwendungsbereich der DSGVO ist nämlich nur bei personenbezogenen, nicht aber bei anonymisierten Daten eröffnet.[34] Die Anonymisierung personenbezogener Daten ist aber auch eine Verarbeitung i. S. d Art. 4 Nr. 2 DSGVO, sodass eine Rechtsgrundlage nach der DSGVO erforderlich ist.[35] Um personenbezogene Daten zu anonymisieren, kommt als Rechtsgrundlage eine Einwilligung nach Art. 6 Abs. 1 S. 1. lit. a DSGVO in Betracht. Es wird indes schwierig umzusetzen sein, bei einer Vielzahl von Personen die Einwilligung für eine Anonymisierung einzuholen. Alternativ können Art. 6 Abs. 1 S. 1. lit. f DSGVO oder Art. 6 Abs. 1 S. 1 lit. c DSGVO i. V. m. Art. 17 DSGVO als Rechtsgrundlage für die Anonymisierung dienen.[36] Voraussetzung ist, dass berechtigte Interessen der betroffenen Person das Interesse der Verantwortlichen an der Anonymisierung nicht

---

[28] Kapitel 6 C.IV (S. 171).
[29] Kapitel 6 D. (S. 204).
[30] S. Kapitel 6 (S. 97).
[31] Kapitel 6 B. (S. 117).
[32] Kapitel 6 C. (S. 161).
[33] Kapitel 6 D. (S. 204).
[34] Kapitel 6 B.II. (S. 121).
[35] Kapitel 6 B.II.3. (S. 123).
[36] Kapitel 6 B.II.3. (S. 123).

überwiegen. Das Interesse, dass die personenbezogenen Daten nicht anonymisiert werden sollen, überwiegt richtigerweise nicht, wenn keine Gefahr für die betroffene Person mehr besteht, also eine Re-Identifikation ausgeschlossen ist. In solchen Fällen kann das Anonymisieren mit dem Löschen gleichgesetzt werden, sodass Art. 6 Abs. 1 S. 1. lit. c DSGVO i. V. m. Art. 17 DSGVO als Rechtsgrundlage für das Anonymisieren herangezogen werden kann.[37]

13. Trainiert man das System mit personenbezogenen Daten, kann der Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO als Rechtsgrundlage dienen. Art. 6 Abs. 4 DSGVO ist nach hier vertretener Ansicht eine eigene Rechtsgrundlage, sodass bei Vorliegen der Voraussetzungen des Kompatibilitätstests eine Verarbeitung zu einem anderen Zweck als dem ursprünglichen Zweck möglich ist. [38] Die Voraussetzungen des Kompatibilitätstests sind hoch, da personenbezogene Daten grundsätzlich nur für die vorher festgelegten Zwecke (Art. 5 Abs. 1 lit. b DSGVO) verarbeitet werden dürfen. Für das Training algorithmischer Systeme kommt eine Weiterverarbeitung nach den Kriterien des Art. 6 Abs. 4 DSGVO insbesondere in Betracht, wenn geeignete Garantien für den Schutz personenbezogener Daten vorhanden sind. [39] Die Möglichkeit der Weiterverarbeitung zu anderen Zwecken ist mithin stark von technisch möglichen Schutzmaßnahmen abhängig.

14. Trainiert man das algorithmische System mit personenbezogenen Daten, die man aufgrund einer Einwilligung nach Art. 6 Abs. 1 S. 1. lit. a DSGVO verarbeitet, muss die Einwilligung freiwillig erteilt werden. Das Merkmal der Freiwilligkeit ist beim bloßen Training eines algorithmischen Systems weniger problematisch als beim konkreten Einsatz des Systems: Es geht noch nicht um ein *konkretes* Arbeitsverhältnis, sodass sich die betroffene Person nicht unbedingt in einem Abhängigkeitsverhältnis zur Verantwortlichen befindet. Eine andere Situation liegt aber vor, wenn die Einwilligung zur Verwendung der Daten als Trainingsdaten in Zusammenhang mit z. B. der

[37] Kapitel 6 B.II.3.c) (S. 129).
[38] Kapitel 6 B.IV.1. (S. 133).
[39] Kapitel 6 B.IV.4.e) (S. 142).

Bewerbung eingeholt wird.[40] In einem solchen Fall wird es in der Regel an der Freiwilligkeit fehlen.

15. Die betroffene Person kann die Einwilligung jederzeit widerrufen. In diesem Fall ist die Verantwortliche gem. Art. 17 Abs. 1 lit. b DSGVO verpflichtet, die betroffenen Daten zu löschen. Das kann im Extremfall dazu führen, dass das ganze System in der Form nicht mehr verwendet werden darf. Etwas anderes gilt nur dann, wenn für die betroffene Person kein Risiko einer Identifikation mehr besteht. Grundsätzlich ist das fertig trainierte System an sich nicht mehr personenbezogenen. Ist ausgeschlossen, dass mittels technischer Möglichkeiten der Personenbezug wiederhergestellt werden kann, darf das System auch weiterhin verwendet werden.[41]

16. Verarbeitet man die personenbezogenen Daten zu Trainingszwecken auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f DSGVO, ist es ein milderes Mittel gegenüber der Verarbeitung personenbezogener Daten, wenn die Daten pseudonymisiert verarbeitet werden.[42] Außerdem dürfen die Interessen der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, das Interesse an der Verarbeitung nicht überwiegen. Das Interesse an der Verarbeitung überwiegt, wenn geeignete Schutzmaßnahmen für die relevanten Daten getroffen wurden: Wie auch bereits im Rahmen von Art. 6 Abs. 4 DSGVO dargelegt, hängt das Ergebnis der Abwägung nach Art. 6 Abs. 1 lit. f. DSGVO somit ebenfalls maßgeblich von den technischen Vorkehrungen ab, die die Verantwortliche trifft.

17. Werden algorithmische Systeme im Rahmen eines *konkreten* Bewerbungs- oder Beschäftigungsverhältnisses eingesetzt, richtet sich die Verarbeitung der personenbezogenen Daten vorrangig nach Art. 6 Abs. 1 S. 1 lit. b DSGVO.[43] Bis auf § 26 Abs. 1 S. 1 BDSG ist § 6 BDSG weiterhin anwendbar, sodass die Vorgaben entsprechend im

---

[40] S. Kapitel 6 B.V.2.b) (S. 147).
[41] Kapitel 6 B.V.3. (S. 151).
[42] Kapitel 6 B.VI.2.b) (S. 158).
[43] Kapitel 6 C.IV. (S. 171).

Beschäftigungskontext berücksichtigt werden müssen.[44] Nach § 26 Abs. 2 BDSG kann die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses einwilligen. Wie auch im Rahmen der Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO muss die betroffene Person die Einwilligung insbesondere freiwillig erteilen. Im Arbeitsverhältnis herrscht typischerweise ein Ungleichgewicht, weil die Beschäftigten und Bewerberinnen sich in einer Abhängigkeitssituation befinden.[45] Dennoch ist eine Einwilligung im Beschäftigungsverhältnis nicht zwingend ausgeschlossen:[46] Als Abwägungskriterium muss auch die individuelle Situation der betroffenen Person miteinbezogen werden. Wenn eine Bewerbung beispielsweise nur eine von vielen ist und die Person bereits Zusagen von anderen Arbeitgeberinnen erhalten hat oder ihre Position auf dem Arbeitsmarkt unabhängig davon hervorsticht, kann eine Einwilligung trotz des im Bewerbungsstadiums bestehenden Drucks freiwillig erteilt werden. Für die Arbeitgeberin wird es aber schwierig sein, zu beweisen, dass in einem solchen Fall die Einwilligung auch tatsächlich freiwillig erteilt wurde. Sie weiß insbesondere auch nicht, ob die Person bereits von anderen Arbeitgeberinnen Zusagen erhalten hat oder wie die Position der Bewerberin auf dem Arbeitsmarkt zu beurteilen ist.

18. Nach Art. 6 Abs. 1 S. 1 lit. b DSGVO dürfen personenbezogene Daten verarbeitet werden, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Die Verarbeitung personenbezogener Daten mittels algorithmischer Systeme müsste daher zur Erfüllung des Arbeitsvertrags erforderlich sein. Wie auch im Rahmen von § 26 Abs. 1 S. 1 BDSG ist im Rahmen der Erforderlichkeitsprüfung nach Art. 6 Abs. 1 S. 1 lit. b DSGVO eine Verhältnismäßigkeitsprüfung vorzunehmen[47]: Dabei muss ein System

---

[44] Kapitel 5 B.II.1.d) (S. 92); Kapitel 6 C.III. (S. 163).
[45] Kapitel 6 C.III.1. (S. 163).
[46] Kapitel 6 C.III.1. (S. 163).
[47] Kapitel 6 C.IV.2. (S. 172).

auf Ebene der Geeignetheit [48] insbesondere eine hohe Qualität der Trainingsdaten aufweisen, damit sachfremde Erwägungen nicht mit in das Ergebnis einfließen. Zudem darf das System nur zulässige Fragen in Bezug auf die konkrete Tätigkeit stellen. Es darf die Person mithin auch nicht auf Merkmale hin analysieren, die für die relevante Tätigkeit nicht von Belang sind.

19. Auf Ebene der Erforderlichkeit im engeren Sinne darf es kein milderes, gleich geeignetes Mittel geben. [49] Je nach Ausgestaltung kann ein algorithmisches System gegenüber herkömmlichen Auswahlverfahren sogar milder sein. Das ist insbesondere der Fall, wenn man mit dem algorithmischen System „üben" kann, indem man Probeläufe absolviert, bevor man eine konkrete Antworten hochlädt und abschickt. Sofern ein milderes Mittel vorliegt, muss dieses auch gleich geeignet sein. [50] Die gleiche Eignung ist sowohl in quantitativer als auch in qualitativer Hinsicht zu beurteilen. In quantitativer Hinsicht sind algorithmische Systeme besser geeignet, wenn eine Vielzahl an Daten ausgewertet werden soll. Das ist für eine menschliche Entscheidungsperson nicht ohne Weiteres möglich. [51] In qualitativer Hinsicht kann man mithilfe algorithmischer Entscheidungen das risikobehaftete, subjektive Gefühl von Personalerinnen außer Acht lassen. Die Entscheidung kommt bei algorithmischen Systemen aufgrund (teilweise) nachprüfbarer Parameter zustande.

20. Zuletzt muss der Einsatz eines algorithmischen Systems auch angemessen sein. [52] Dabei sind das Interesse der Arbeitgeberin an der Datenverarbeitung und das Persönlichkeitsrecht der betroffenen Person gegeneinander abzuwägen. Bei der Angemessenheitsprüfung müssen verschiedene Abwägungskriterien berücksichtigt werden. Auf Seiten der Arbeitgeberin ist insbesondere zu berücksichtigen, für welche Zwecke und in welchem Kontext sie das algorithmische System einsetzt.

---

[48] Kapitel 6 C.IV.2.b) (S. 176).
[49] Kapitel 6 C.IV.2.c) (S. 178).
[50] Kapitel 6 C.IV.2.c)bb) (S. 181).
[51] Vgl. dazu bereits: Kapitel 3 B. (S. 35).
[52] Kapitel 6 C.IV.2.d) (S. 182).

Die Datenverarbeitung mittels algorithmischer Systeme ist eher angemessen, wenn die Arbeitgeberin eine objektive Auswahlentscheidung herbeiführen will oder ansonsten der Menge der Daten nicht gerecht wird. Zu berücksichtigen ist auf Seiten der Arbeitnehmerin, dass sie nicht permanent überwacht werden darf, eine umfassende Persönlichkeitsprofilerstellung unzulässig ist und der Person nicht ihre Individualität abgesprochen werden darf. Letzteres ist der Fall, wenn Erfolgschancen im Beruf sowie mögliche Kündigungsabsichten auf der Grundlage von Gestik oder Mimik bewertet werden.[53] Menschliches Verhalten wird dadurch berechenbar gemacht, sodass das Individuum mit seinen Persönlichkeitsfacetten in den Hintergrund gerät. Eine solche „Katalogisierung" der individuellen Persönlichkeit ist nicht mit der Menschenwürde gem. Art. 1 GRCh vereinbar.

21. Als weitere Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext kommt eine Betriebsvereinbarung in Betracht (Art. 88 DSGVO).[54] Dabei können die Betriebsparteien vom Schutzstandard des Art. 88 Abs. 2 DSGVO sowohl „nach oben" als auch – nach hier vertretener Ansicht – in den Grenzen des Art. 88 Abs. 2 DSGVO „nach unten" abweichen.[55] Sie müssen insoweit Art. 5, 6 und 9 DSGVO einhalten und Art. 12 ff. DSGVO berücksichtigen. Das schließt aber nicht aus, dass die Arbeitgeberin und der Betriebsrat eine für ihre betriebliche Situation angemessene und individuell austarierte Vereinbarung abschließen, die als Rechtsgrundlage für die Datenverarbeitung dient.

D. Verbot ausschließlich automatisierter Entscheidungen

22. Werden die Ergebnisse des algorithmischen Systems verwendet, müssen die Voraussetzungen des Art. 22 DSGVO gewahrt werden.[56] Gem.

---

[53] Kapitel 6 C.IV.2.d)aa)(6) (S. 188).
[54] Kapitel 6 C.V.1. (S. 193).
[55] Kapitel 6 C.V.2.a)cc) (S. 198).
[56] Kapitel 6 D. (S. 204).

Art. 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Art. 22 DSGVO ist neben Art. 6 und 9 DSGVO sowie § 26 BDSG anwendbar.[57]

23. Das Merkmal der „Entscheidung" i. S. d. Art. 22 Abs. 1 DSGVO ist teleologisch auf solche Fälle zu reduzieren, die ein Mindestmaß an Komplexität aufweisen. Das ist insbesondere bei maschinell lernenden Systemen der Fall, die eine eigene Bewertung vornehmen. Trifft ein nicht-lernendes System eine Entscheidung anhand klar vorgegebener Regeln, würde der Mensch in Anwendung entsprechender Regeln zu keinem anderen Ergebnis kommen als die Maschine.[58] Der auf die Gefahren einer automatisierten Entscheidung abzielende Schutzzweck des Art. 22 Abs. 1 DSGVO greift dann nicht. In solchen Fällen liegt keine „Entscheidung" i. S. d. Art. 22 Abs. 1 DSGVO vor.

24. Bei algorithmischen Systemen, die nur eine Vorauswahl treffen, ist Art. 22 Abs. 1 DSGVO nicht einschlägig: Die Letztentscheidung liegt beim Menschen, sodass keine *ausschließlich* automatisierte Verarbeitung vorliegt. Der Mensch muss aber eigene Erwägungen anstellen und darf das Ergebnis des Systems nicht ohne eigene Abwägung übernehmen.[59]

25. Um nachzuvollziehen, dass eine eigene Entscheidung getroffen wurde, schlägt diese Arbeit eine Protokollpflicht vor.[60] Die jeweilige menschliche Entscheidungsträgerin könnte etwa anhand eines Fragebogens beantworten, wie sie die Entscheidung getroffen hat. Für eine objektive Dritte muss aus den Ausführungen hervorgehen, dass eigene Überlegungen mit in die Entscheidung eingeflossen sind. Mit

---

[57] Kapitel 6 D. (S. 204).
[58] Kapitel 6 D.IV.1. (S. 211).
[59] Kapitel 6 D.IV.3.a) (S. 212).
[60] Kapitel 6 D.IV.3.c) (S. 219).

einem derartigen Protokoll kann die entsprechende verantwortliche Person ein algorithmisches System rechtssicher implementieren.

26. Von dem grundsätzlichen Verbot ausschließlich automatisierter Entscheidungen in Art. 22 Abs. 1 DSGVO gibt es nach Art. 22 Abs. 2 DSGVO Ausnahmen. Liegen die Voraussetzungen von Art. 22 Abs. 2 lit. a, b oder c DSGVO vor, ist eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung zulässig. Im Beschäftigungskontext kommt nur die Ausnahme nach Art. 22 Abs. 2 lit. a DSGVO in Betracht.[61] Nach Art. 22 Abs. 2 lit. a DSGVO gilt Art. 22 Abs. 1 DSGVO nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und der Verantwortlichen erforderlich ist. Eine ausschließlich automatisierte Entscheidung ist gem. Art. 22 Abs. 2 lit. a DSGVO erforderlich, wenn eine menschliche oder eine Kombination aus maschineller und menschlicher Entscheidung nicht realisierbar ist.[62] Das wiederum setzt voraus, dass im Hinblick auf eine Vielzahl von Daten eine Entscheidung innerhalb einer kurzen Zeitspanne getroffen werden muss. Das Merkmal der Erforderlichkeit i. S. d. Art. 22 Abs. 2 lit. a DSGVO ist vor diesem Hintergrund erfüllt, wenn die Arbeitgeberin die Daten einer Bewerberin sonst gar nicht auswerten würde, weil ihr das in Anbetracht der Datenmenge und der zeitlichen Vorgabe nicht möglich ist.

E. Anforderungen nach dem AGG

27. Wird ein algorithmisches System im Bewerbungsverfahren oder im bestehenden Arbeitsverhältnis eingesetzt, ist der Anwendungsbereich des AGG in sachlicher und in persönlicher Hinsicht eröffnet.[63] Werden im Bewerbungsverfahren Daten gesammelt, um ein maschinell lernendes System zu trainieren, welches im nächsten Bewerbungsprozess eingesetzt werden soll, geht es um Szenarien, die in den

[61] Kapitel 6 D.IV.5.b) (S. 229); Kapitel 6 D.IV.5.c) (S. 230).
[62] Kapitel 6 D.IV.5.a)bb) (S. 225).
[63] Kapitel 9 A.I. (S. 293).

Anwendungsbereich des AGG fallen können. In solchen Fällen ist der Anwendungsbereich des AGG bereits bei der Sammlung von Trainingsdaten eröffnet.[64] Das maschinell lernende System legt dann Bedingungen fest, die für den Zugang zu unselbständiger und selbständiger Erwerbstätigkeit relevant sind (§ 2 Abs. 1 Nr. 1 AGG). Bereits gegen eine potenzielle Benachteiligung wegen unzureichender Trainingsdaten vorzugehen, ist in Deutschland aber bislang nicht möglich, weil es auf nationaler Ebene keine Verbandsklage zur Durchsetzung des AGG in Fällen potenzieller Benachteiligungen gibt.

28. Algorithmische Systeme können aus verschiedenen Gründen eine unmittelbare (§ 3 Abs. 1 AGG) oder mittelbare Benachteiligung (§ 3 Abs. 2 AGG) hervorrufen.[65]

29. Eine unmittelbare Benachteiligung liegt vor, wenn eine Person wegen eines in § 1 AGG genannten Grundes eine weniger günstige Behandlung erfährt, als eine andere Person in einer vergleichbaren Situation erfährt, erfahren hat oder erfahren würde (§ 3 Abs. 1 AGG). Anknüpfungspunkt der Benachteiligung ist dabei nicht die Behandlung durch das algorithmische System selbst, sondern die menschliche Letztentscheidung, die wegen Art. 22 DSGVO erforderlich ist.[66]

30. Bei einem nicht-lernenden System ist eine unmittelbare Benachteiligung denkbar, da die Auswahlkriterien bewusst durch die Entwicklerinnen in das System einprogrammiert werden.[67]

31. Bei maschinell lernenden Systemen wird es eher zu mittelbaren Benachteiligungen kommen. Eine mittelbare Benachteiligung liegt gem. § 3 Abs. 2 AGG vor, wenn dem Anschein nach neutrale Vorschriften, Kriterien oder Verfahren Personen wegen eines in § 1 AGG genannten Grundes gegenüber anderen Personen in besonderer Weise benachteiligen. Die verwendeten Kriterien und Parameter des

---

[64] Kapitel 9 A.I.2. (S. 294).
[65] S. Kapitel 8 B. (S. 288).
[66] Kapitel 9 A.II.1.a) (S. 296).
[67] Kapitel 8 B.III. (S. 290).

maschinell lernenden Systems, die der Entscheidung zugrunde liegen, sind an sich neutral. Wegen unzutreffender Korrelationen können sich mittelbare Benachteiligungen ergeben.[68] Außerdem kann es sein, dass die Trainingsdatenqualität mangelhaft ist. So können sich in den Trainingsdaten angelegte Vorurteile und Diskriminierungen in den Entscheidungsparametern des fertig trainierten algorithmischen Systems niederschlagen.[69]

32. Der Vorschlag von *Spiecker gen. Döhmann* und *Towfigh*, den Anwendungsbereich des § 1 AGG auch auf eine Benachteiligung zu erstrecken, die sich „aus einer Beziehung ergibt, die nur auf statistischer Korrelation beruht", ist abzulehnen.[70] Insbesondere fehlt einem solchen Benachteiligungsmerkmal der materielle Charakter der sonstigen in § 1 AGG genannten Merkmale, weil sich der Vorschlag nicht auf den Entscheidungsgrund, sondern das Entscheidungsverfahren bezieht.

33. Gem. § 7 AGG muss die Benachteiligung *wegen* eines in § 1 AGG genannten Merkmals erfolgen (Kausalität).[71] Dabei reicht es aus, wenn die Benachteiligung wegen mehrerer Merkmale (sog. Motivbündel) erfolgt. Da maschinell lernende Systeme mit vielen Daten trainiert werden, wird die Benachteiligung eher nicht nur auf einem Merkmal beruhen.[72] Die Kausalität entfällt nicht deshalb, weil die Entscheidungsträgerin keine Kenntnis der diskriminierenden Parameter hat. Sie macht sich das Ergebnis des Systems zu eigen, indem sie es in ihre Entscheidung mit einbezieht.

34. Eine unmittelbare Benachteiligung kann im Einzelfall nach §§ 8-10 AGG gerechtfertigt sein. Wenn der Einsatz eines algorithmischen Systems eine positive Maßnahme i. S. d. § 5 AGG ist, kommt auch eine Rechtfertigung nach § 5 AGG in Betracht. Eine solche positive Maßnahme liegt vor, wenn das algorithmische System z. B. konkret für

---

[68] Kapitel 8 B.II. (S. 289).
[69] Kapitel 8 B.I. (S. 288).
[70] Kapitel 9 A.II.1.b) (S. 298).
[71] Kapitel 9 A.II.1.c) (S. 298).
[72] Kapitel 9 A.II.2. (S. 301).

den Anwendungsfall trainiert worden ist, Ziele wie etwa das Geschlechtergleichgewicht in einem Unternehmen zu verbessern.

35. Eine mittelbare Benachteiligung ist gem. § 3 Abs. 1 Hs. 2 AGG gerechtfertigt, wenn die Vorschriften, Kriterien oder Verfahren, die zu einer mittelbaren Benachteiligung führen, durch ein rechtmäßiges Ziel sachlich gerechtfertigt und die Mittel zur Erreichung des Ziels erforderlich und angemessen sind. Die Arbeitgeberin verfolgt in aller Regel ein legitimes Ziel mit dem Einsatz des algorithmischen Systems.[73] Ein solches Ziel liegt etwa darin, die geeignete Kandidatin für eine zu besetzende Stelle zu finden. Das algorithmische System ist grundsätzlich geeignet, das legitime Ziel zu erreichen, wenn es entsprechende Test- und Validierungsverfahren durchlaufen hat und die Arbeitgeberin zudem nachweisen kann, dass die Qualität der Trainingsdaten nach Art. 10 Abs. 5 KI-VO-KOM[74] sichergestellt ist.[75]

36. Auf der Ebene der Erforderlichkeit ist zu prüfen, ob es ein gleich geeignetes, milderes Mittel gegenüber dem Einsatz eines algorithmischen Systems gibt.[76] Herkömmliche Verfahren zur Bewerberinnenauswahl oder auch zur Auswahl von Personen, die befördert werden sollen, sind – wie auch bereits im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO deutlich wird – nicht unbedingt milder gegenüber der Auswahl durch algorithmische Systeme, wenn letztere z. B. Probeläufe ermöglichen.[77]

37. Vorausgesetzt, es gibt kein gleich geeignetes, milderes Mittel, muss der Einsatz des Systems auch angemessen sein.[78] Das bedeutet, dass das System die legitimen Interessen der Personen nicht übermäßig beeinträchtigen darf, die wegen eines in § 1 AGG genannten Grundes mittelbar benachteiligt werden. Die Gründe einer mittelbaren

---

[73] Kapitel 9 A.III.2.a) (S. 304).
[74] Kapitel 10 B.I. (S. 345).
[75] Kapitel 9 A.III.2.b)aa) (S. 304).
[76] Kapitel 9 A.III.2.b)bb) (S. 306).
[77] S. dazu bereits Kapitel 6 C.IV.2.c)aa) (S. 178).
[78] Kapitel 9 A.III.2.b)cc) (S. 307).

Benachteiligung sind häufig auf ein unzureichendes Trainingsdatenset zurückzuführen. Im Rahmen der Angemessenheitsprüfung ist zu berücksichtigen, dass die Arbeitgeberin erstens im Regelfall die Kosten für ein qualitativ höherwertigeres und somit weniger zu Benachteiligungen führendes Trainingsdatenset aufzuwenden hat.[79] Wenn keine besseren Trainingsdaten verfügbar sind oder es mit unverhältnismäßigen Kosten verbunden wäre, bessere Trainingsdaten zu beschaffen, ist das System zweitens nur angemessen, wenn die Arbeitgeberin nachweist, dass das eingesetzte System signifikant und nachweislich zu weniger voreingenommen Ergebnissen kommt als andere (nicht algorithmische) Verfahren.

38. Die Arbeitgeberin haftet bei Verstößen gegen das Benachteiligungsverbot nach § 15 Abs. 1 S. 1 AGG oder § 15 Abs. 2 S. 1 AGG. § 15 Abs. 1 AGG setzt ein Vertretenmüssen der Arbeitgeberin voraus (§ 15 Abs. 1 S. 2 AGG), für dessen Fehlen die Arbeitgeberin darlegungs- und beweispflichtig ist.[80] Das Vertretenmüssen richtet sich nach §§ 276 ff. BGB. Beim Umfang des Vertretenmüssens ist zu berücksichtigen, welches Wissen die Arbeitgeberin über das algorithmische System hat.[81] Grundsätzlich muss sich die Arbeitgeberin nach den Grundsätzen der Wissenszurechnung das Wissen über den *Output* (Ergebnis des Systems) und teilweise auch über den *Input* (insbesondere die Trainingsdaten) zurechnen lassen. Ergibt sich aufgrund dieses Wissens, dass die Arbeitgeberin durch den Einsatz des Systems die im Verkehr erforderliche Sorgfalt außer Acht lässt, handelt sie fahrlässig und hat den Verstoß gegen das Benachteiligungsverbot nach § 15 Abs. 1 S. 1 AGG zu vertreten.[82] Nicht zuzurechnen ist der Arbeitgeberin aber das implizite Wissen, also die Vorgänge im „Inneren" des maschinell lernenden Systems. Das sind regelmäßig die vom System vorgenommenen Gewichtungen einzelner Parameter.

---

[79] S. Kapitel 9 A.III.2.b)cc) (S. 307).
[80] Kapitel 9 B.I.1. (S. 310).
[81] S. Kapitel 9 B.I.1.a) (S. 311).
[82] Kapitel 9 B.I.1.a) (S. 311).

39. Handelt die Herstellerin fahrlässig, wird das Verschulden der Herstellerin der Arbeitgeberin gem. § 278 S. 1 BGB zugerechnet.[83] Die Arbeitgeberin hat gem. § 12 Abs. 1 AGG die Pflicht, Maßnahmen zum Schutz vor Benachteiligungen zu treffen. Das umfasst im Kontext algorithmischer Systeme auch, dass sie sicherstellen muss, dass keine diskriminierenden Parameter verwendet werden. Indem sie die Pflicht auf die Herstellerin des Systems überträgt, die die technischen Prüfverfahren durchführt und sicherstellt, dass das System keine Benachteiligungen hervorruft, setzt sie die Herstellerin als Erfüllungsgehilfin ein.

40. § 278 S. 1 BGB ist nicht analog auf algorithmische Systeme selbst anzuwenden, da für eine solche Analogie kein Bedarf besteht.[84] Eine Regelungslücke besteht schon deshalb nicht, weil Arbeitgeberin und die Herstellerin das System auf eine mögliche mittelbare Benachteiligung hin überprüfen und entsprechende Vorkehrungen treffen müssen. Tun sie das nicht, haftet die Arbeitgeberin entweder direkt oder ihr wird – wie soeben ausgeführt – das Verschulden der Herstellerin über § 278 S. 1 BGB zugerechnet. Außerdem kann ein algorithmisches System nicht die im Verkehr erforderliche Sorgfalt außer Acht lassen und daher nicht schuldhaft handeln. Es fehlt somit an einer vergleichbaren Interessenlage.

41. Der Anspruch nach § 15 Abs. 1 S. 1 AGG scheitert in der Praxis fast immer, weil die Bewerberin darlegen und beweisen müsste, dass sie die am besten geeignete Kandidatin für die Position gewesen wäre. Dieser Nachweis wird ihr kaum gelingen.[85]

42. Praxisrelevanter ist daher der verschuldensunabhängige Anspruch auf angemessene Entschädigung nach § 15 Abs. 2 S. 1 AGG. [86] Die Anspruchstellerin muss im Schadensersatzprozess als nach den allgemeinen Grundsätzen darlegungs- und beweisbelastete Partei

---

[83] Kapitel 9 B.I.1.b) (S. 314).
[84] Kapitel 9 B.I.2. (S. 316).
[85] Kapitel 9 B.I.3. (S. 318).
[86] Kapitel 9 B.II. (S. 318).

Indizien vortragen, die auf eine Benachteiligung i. S. d. AGG schließen lassen. Zwar statuiert § 22 AGG eine Beweiserleichterung: Beweist die eine Partei Indizien, die eine Benachteiligung wegen eines in § 1 AGG genannten Grundes vermuten lassen, trägt die andere Partei die Beweislast dafür, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligungen vorgelegen hat. Diese wird bei algorithmischen Systemen aber kaum weiterhelfen, weil die Anspruchstellerin zumeist keinen näheren Einblick in das System hat. Damit § 22 AGG im Kontext algorithmischer Systeme seinen Normzweck erfüllt, muss das von *Grünberger* entwickelte Zwei-Stufen-Modell der Darlegungslast greifen.[87] Bei diesem Modell handelt es sich eigentlich um ein Vier-Stufen-Modell. Die Bewerberin genügt auf der ersten Stufe ihrer Darlegungslast, wenn sie darlegt, dass ein algorithmisches System eingesetzt wurde. Auf der zweiten Stufe muss die Arbeitgeberin darlegen, dass das System den technischen Fairnessanforderungen genügt, etwa, ob die Anforderungen an das Hochrisiko-KI-System nach dem KI-VO-KOM gewahrt wurden. Widerlegt die Bewerberin auf der dritten Stufe die Vermutung, dass keine Benachteiligung vorliegt, muss die Arbeitgeberin auf der vierten Stufe das System und die Entscheidung offenlegen. Das Modell schafft einen angemessenen Ausgleich zwischen den Interessen der Bewerberin und der Arbeitgeberin, da mit jeder Stufe die Anforderungen an die Darlegungslast für beide Seiten erhöht werden.

F. Anforderungen nach einer zukünftigen KI-VO

43. Am 21. April 2021 hat die Europäische Kommission den KI-VO-KOM vorgelegt. Am 6. Dezember 2022 hat der Rat den KI-VO-RAT veröffentlicht, der sich teilweise vom Vorschlag der Kommission unterscheidet. Stärker noch als der KI-VO-RAT unterscheidet sich der KI-VO-PARL vom KI-VO-KOM, den das Europäische Parlament am 14. Juni 2023 angenommen hat. Bislang haben sich die Kommission, der

[87] Kapitel 9 B.II.1.c) (S. 321).

Rat der Europäischen Union und das Parlament noch nicht auf einen finalen Gesetzestext geeinigt.[88]

44. Der KI-VO-KOM ist sachlich auf KI-Systeme anwendbar.[89] Nach der in Art. 3 Nr. 1 KI-VO-KOM aufgeführten Definition ist ein KI-System eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf verschiedene vom Menschen festgelegte Ziele Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld, mit dem sie interagieren, beeinflussen. Diese Definition wird im KI-VO-RAT eingegrenzt: Nach Ansicht des Rats sollten KI-Systeme solche Systeme sein, die anhand von Konzepten des maschinellen Lernens sowie logik- und wissensgestützten Konzepten entwickelt wurden und mit Elementen der Autonomie arbeiten. Offen bleibt aber, was unter „Elemente der Autonomie" genau verstanden wird. Der KI-VO-PARL differenziert zudem zwischen einem sog. *foundation model* (Basismodell), einem sog. *general purpose AI system* (KI-System für allgemeine Zwecke) und einer sog. *generative AI* (generative KI).[90] Diese Differenzierung ist zu begrüßen, weil dadurch auch generative KI-Systeme wie *ChatGPT* erfasst werden, für die der KI-VO-KOM keine besonderen Regelungen vorsieht. Allerdings ist eine trennscharfe Abgrenzung zwischen den drei genannten Systemen kaum möglich. Ein Basismodell wird in der Regel auch ein generatives KI-System sein. Häufig wird es gleichzeitig auch ein KI-System für allgemeine Zwecke sein. Jedenfalls erfüllt der Begriff des KI-Systems für allgemeine Zwecke keinen eigenen Mehrwert, weil ein KI-System für allgemeine Zwecke zumeist auch ein generatives KI-System ist. Der Begriff des KI-Systems für allgemeine Zwecke sollte daher aufgegeben werden.

45. Der KI-VO-KOM richtet sich gem. Art. 2 Abs. 1 KI-VO-KOM an Anbieterinnen und Nutzerinnen,[91] wobei die meisten Pflichten erstere treffen. Anbieterin ist eine Person, die ein KI-System entwickelt oder

---

[88] Kapitel 5 A.IV.1. (S. 74).
[89] Kapitel 5 A.IV.3.a) (S. 77).
[90] Kapitel 5 A.IV.3.a) (S. 77).
[91] Kapitel 5 A.IV.3.b) (S. 79); Kapitel 10 A. (S. 341).

entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen. Darunter fällt typischerweise die Entwicklerin des KI-Systems. Die Arbeitgeberin, die das KI-System im eigenen Unternehmen einsetzt, ist hingegen keine Anbieterin, sondern regelmäßig die Nutzerin gem. Art. 2 Nr. 4 KI-VO-KOM. Der Begriff der Nutzerin wird im KI-VO-PARL sinnvollerweise in den Begriff Bereitstellerin geändert. So kommt es nicht zu Verwechselungen, wenn man diejenigen Personen bezeichnen möchte, die ein KI-System als Endnutzerinnen direkt verwenden. Im KI-VO-PARL wird jedoch der Begriff der Nutzerin weiter verwendet, obwohl er nicht mehr definiert wird. Die finale KI-VO sollte für alle drei Akteurinnen – Anbieterinnen, Bereitstellerinnen und Nutzerinnen – eine Definition bereithalten, damit man klar abgrenzen kann.

46. Sowohl im KI-VO-KOM als auch im KI-VO-RAT und KI-VO-PARL erfolgt eine Einteilung von KI-Systemen nach Risikogruppen.[92] Die Entwicklung und der Einsatz von KI-Anwendungen sind je nach Risikostufe unterschiedlich streng reguliert. Der KI-VO-KOM unterscheidet zwischen drei Kategorien: KI-Systemen mit a) unannehmbaren Risiken, b) hohen Risiken und c) geringen oder minimalen Risiken. Die hier untersuchten algorithmischen Systeme fallen gem. Annex III Nr. 4 KI-VO-KOM in die Kategorie der Hochrisiko-KI-Systeme.[93]

47. Wenn KI-Systeme mit personenbezogenen Daten trainiert werden, oder wenn fertige KI-Systeme personenbezogene Daten verarbeiten, ist neben einer zukünftigen KI-VO auch die DSGVO einschlägig. Die beiden Regelwerke sollen sich ausweislich des KI-VO-KOM ergänzen. Das gelingt aber bislang nur teilweise. Zu kritisieren ist insbesondere, dass der KI-VO-KOM es vermeidet, Rechtsgrundlagen für bestimmte Verarbeitungszwecke zu schaffen. Gem. Art. 10 Abs. 5 KI-VO-KOM dürfen personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO verarbeitet werden, soweit dies für die Beobachtung, Erkennung und Korrektur

[92] Kapitel 5 A.IV.5. (S. 82).
[93] Kapitel 5 A.IV.5. (S. 82).

von Verzerrungen im Zusammenhang mit Hochrisiko-Systemen unbedingt erforderlich ist. Obwohl Art. 10 Abs. 5 KI-VO-KOM[94] als Ausnahme zu Art. 9 Abs. 2 lit. g DSGVO einzuordnen ist, soll Art. 10 Abs. 5 KI-VO-KOM ausweislich des Erwägungsgrundes 41 KI-VO-KOM keine eigenständige Rechtsgrundlage sein. Richtigerweise ist Art. 10 Abs. 5 KI-VO-KOM aber als Rechtsgrundlage einzuordnen. Vor diesem Hintergrund ist es zu begrüßen, dass in Erwägungsgrund 41 KI-VO-PARL der entscheidende Satz gestrichen wurde, der gegen die Einordnung als Rechtsgrundlage gesprochen hätte. Art. 10 Abs. 5 KI-VO-PARL ist somit in jedem Fall als Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten einzustufen.[95]

48. Art. 10 Abs. 5 KI-VO-KOM soll die Beobachtung, Erkennung und Korrektur von Verzerrungen (*bias)* ermöglichen.[96] Unter *bias* i. S. d. Art. 10 Abs. 5 KI-VO-KOM sollte grundsätzlich eine diskriminierende oder sonst benachteiligende Entscheidung gegenüber einer Person durch ein KI-System verstanden werden. Man sollte sich an den Fallgruppen des AGG orientieren, die aber nicht abschließend zu verstehen sind. Mögliche Verzerrungen in KI-Systemen sollten nicht nur dann erfasst werden, wenn sie im AGG genannt sind. Es können dabei alle Formen von *technical bias*, *pre-existing bias* und *emergent bias* erfasst sein. Diese Kategorien können helfen, die unterschiedlichen *biases* einzuordnen. Anders als in Art. 10 Abs. 5 KI-VO-PARL angedeutet, sollten auch gerechtfertigte Benachteiligungen als *bias* eingestuft werden. Das liegt daran, dass es im Rahmen von Art. 10 Abs. 5 KI-VO-KOM darum geht, dass zunächst alle Formen von *biases* erkannt werden sollen, um diese aufgrund der Verarbeitung zusätzlicher sensibler Daten zu verhindern oder jedenfalls zu verringern. Die Frage, ob eine Verzerrung ggf. gerechtfertigt ist, ist eine nachgelagerte Frage, die im Rahmen von Art. 10 Abs. 5 KI-VO-KOM nicht relevant ist.

---

[94] Kapitel 11 B. (S. 371).
[95] Kapitel 11 B.III. (S. 376).
[96] Kapitel 11 B.I. (S. 372).

49. Der Anwendungsbereich eines zukünftigen Art. 10 Abs. 5 KI-VO sollte sich – anders als in allen drei Entwürfen vorgesehen – nicht nur auf Hochrisiko-KI-Systeme beschränken, weil auch bei anderen KI-Systemen Verzerrungen hervorgerufen werden können, die ggf. mithilfe der Verarbeitung sensibler Daten korrigiert werden können.[97]

50. Nach Art. 54 Abs. 1 KI-VO-KOM dürfen rechtmäßig für andere Zwecke erhobene personenbezogene Daten in einem sog. KI-Reallabor unter bestimmten Voraussetzungen für bestimmte Zwecke weiterverarbeitet werden. Art. 54 Abs. 1 KI-VO-KOM ist ausweislich Erwägungsgrund 72 S. 4 KI-VO-KOM eine Rechtsgrundlage zur Datenverarbeitung. Sowohl nach dem KI-VO-KOM als auch dem KI-VO-PARL soll die Verarbeitung aber „im Einklang" mit Art. 6 Abs. 4 DSGVO erfolgen. Die Formulierung „im Einklang" legt den Schluss nahe, dass zusätzlich die Voraussetzungen des Art. 6 Abs. 4 DSGVO vorliegen müssen. Das überzeugt indes nicht.[98] Art. 6 Abs. 4 DSGVO ist selbst eine eigenständige Rechtsgrundlage. Ausweislich des KI-VO-KOM als auch des KI-VO-PARL ist Art. 54 Abs. 1 KI-VO-KOM ebenfalls eine eigenständige Rechtsgrundlage. Es müssen nicht zwei Rechtsgrundlagen erfüllt sein, um eine Verarbeitung personenbezogener Daten durchzuführen. Selbst wenn man Art. 6 Abs. 4 DSGVO nicht als eigenständige Rechtsgrundlage einordnet, wäre es reiner Formalismus, zusätzlich zu den strengen Voraussetzungen des Art. 54 Abs. 1 einer zukünftigen KI-VO auch noch den Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO durchzuführen.

51. Bei Hochrisiko-KI-Systemen muss ein Risikomanagementsystem nach Art. 9 KI-VO-KOM eingerichtet und aufrechterhalten werden.[99] Diese Pflicht trifft die Anbieterin, also regelmäßig die Entwicklerin des Systems. Die Arbeitgeberin ist als datenschutzrechtlich Verantwortliche zur Durchführung einer DSFA gem. Art. 35 DSGVO verpflichtet, wenn sie das System einsetzt. Die beiden Pflichten richten sich in diesem Fall an unterschiedliche Akteurinnen. Es ist sinnvoll, dass die beiden

[97] Kapitel 11 B.IV. (S. 378).
[98] Kapitel 11 E. (S. 384).
[99] Kapitel 11 A.I. (S. 363).

Pflichten nicht miteinander kombiniert werden, damit die Systematik der DSGVO nicht durchbrochen wird.

52. An anderer Stelle können Synergieeffekte mit der DSFA jedoch genutzt werden.[100] Art. 29a Abs. 6 und Art. 54 Abs. 1c KI-VO-PARL regeln zusätzliche Risikoabwägungen. Nach Art. 29a Abs. 6 KI-VO-PARL muss bei bestimmten Hochrisiko-KI-Systemen eine grundrechtliche Folgenabschätzung vorgenommen werden. Art. 54c Abs. 1c KI-VO-PARL sieht vor, dass es effektive Überwachungsmechanismen geben muss, die prüfen, ob während der *Sandbox*-Experimente hohe Risiken für die Rechte und Freiheiten der betroffenen Personen auftreten können. Anders als der KI-VO-KOM und der KI-VO-RAT verweist der KI-VO-PARL in Art. 29a Abs. 6 und Art. 54 Abs. 1 lit. c KI-VO-PARL zurecht auf Art. 35 DSGVO. Der Verweis hat zur Folge, dass die grundrechtliche Folgenabschätzung im Zusammenhang mit der DSFA nach Art. 35 DSGVO durchgeführt werden soll. Nach Art. 54 Abs. 1 lit. c KI-VO-PARL bewirkt der Verweis, dass die nach der DSFA betroffenen Rechte und Freiheiten in der *regulatory sandbox* berücksichtigt werden sollen. Im Unterschied zu Art. 9 Abs. 1 KI-VO-KOM richten sich die Pflichten nach Art. 29a KI-VO-PARL an die Bereitstellerin und damit auch an die Arbeitgeberin. Diese trifft als Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO zudem die Pflicht aus Art. 35 DSGVO, eine Datenschutzfolgenabschätzung durchzuführen. Die beiden Risikoabwägungen sind somit von der gleichen Person durchzuführen, sodass – wie in Art. 29a Abs. 6 KI-VO-PARL Synergieeffekte – genutzt werden können. Auch in Art. 54 Abs. 1 lit. c KI-VO-PARL ergibt der Verweis auf Art. 35 DSGVO Sinn: In der *regulatory sandbox* soll die Anbieterin gerade die Risiken überwachen, die sie in der DSFA identifiziert hat.

53. Außerdem müssen die Trainings-, Test- und Validierungsdatensätze den Anforderungen nach Art. 10 Abs. 2 bis 5 KI-VO-KOM genügen.[101] Gem. Art. 10 Abs. 3 KI-VO-KOM müssen die Trainingsdaten *relevant, repräsentativ, fehlerfrei* und *vollständig* sein. Nach dem Wortlaut des

---

[100] Kapitel 11 A.II. (S. 368); Kapitel 11 A.III. (S. 370).

[101] Kapitel 10 B.I. (S. 345).

Art. 10 Abs. 3 KI-VO-PARL ändert sich an den vier Merkmalen nichts; allerdings sind diese gemäß Art. 10 Abs. 3 KI-VO-PARL – anders als im KI-VO-KOM – sinnvollerweise einer Abwägung zugänglich: Die Trainingsdaten müssen relevant, *hinreichend repräsentativ*, *angemessen auf Fehler überprüft* und im Hinblick auf den beabsichtigten Zweck *so vollständig wie möglich* sein. Trotz abwägungsoffener Formulierung werden die Vorgaben nur schwierig zu erfüllen sein. Aus Sicht einer zukünftigen KI-VO müssen die Voraussetzungen für das Trainingsdatenset erfüllt sein, *bevor* das System trainiert wird. Es ist schwierig, schon im Voraus abzuschätzen, ob die Daten die genannten Merkmale für den entsprechenden Trainingszweck erfüllen. Mit Inkrafttreten der Regelung wird jedoch der Umgang mit geprüften Datensätzen gefördert, da durch die Vorgaben von Art. 10 einer zukünftigen KI-VO die Möglichkeit genommen wird, große, wenig optimierte Datensätze zu Trainingszwecken zu nutzen. Das ist richtig und wichtig, da unzureichende Trainingsdatensätze Benachteiligungen hervorrufen können.[102]

54. Das Merkmal der *relevanten Datensätze* muss so verstanden werden, dass vermieden werden soll, dass viele Daten zu Trainingszwecken genutzt werden, die an sich nicht für den Trainingszweck geeignet sind. Der eigene Regelungszweck des Merkmals ist unklar, weil Daten, die sich aus technischen oder anderen Gründen nicht zum Training des KI-Systems eignen, ohnehin nicht verarbeitet werden. Außerdem muss – sofern es sich um personenbezogene Trainingsdaten handelt – ohnehin der Grundsatz der Datenminimierung gem. Art. 5 Abs 1 lit. c DSGVO eingehalten werden. Demnach dürfen ohnehin nur relevante Daten für den konkreten Zweck verarbeitet werden, weil die Verarbeitung ansonsten nicht auf das notwendige Maß gem. Art. 5 Abs. 1 lit. c DSGVO beschränkt wäre.

55. Trainingsdaten sind dann *repräsentativ*, wenn bei den für das Training charakteristischen Datenkategorien keine Benachteiligungen angelegt sind. Als Anhaltspunkt für den Begriff der Benachteiligung sollte man

[102] Vgl. Kapitel 8 (S. 281).

das AGG heranziehen. Die im AGG aufgeführten Benachteiligungen sind allerdings nicht abschließend.

56. Ein Datensatz ist *vollständig,* wenn das algorithmische System alle notwendigen Datenkategorien abbildet, um ein bestimmtes Ergebnis zu präsentieren.

57. Beim Merkmal der *Fehlerfreiheit* bleibt unklar, was genau Fehlerfreiheit bedeutet. Ob ein Datum keinen „Fehler" wie etwa Mess- und Festplattenfehler aufweist und ob es sachlich richtig ist, ist nicht anhand eines konkreten Einzeldatums feststellbar.

58. Art. 14 KI-VO-KOM regelt, dass Hochrisiko-Systeme während ihrer Verwendung von natürlichen Personen beaufsichtigt werden sollen (Art. 14 Abs. 1 KI-VO-KOM). Die Norm muss sich stärker an Art. 22 DSGVO orientieren[103]: Art. 14 KI-VO-KOM sollte nicht jede Art der Entscheidung – ob vollständig oder unterstützend – erfassen. Wenn ohnehin am Ende ein Mensch die Entscheidung trifft, überzeugt es nicht, warum das System im laufenden Prozess gestoppt werden soll. Zwar bessert Art. 14 KI-VO-PARL in einigen Punkten nach und konkretisiert etwa, dass die Aufsichtspersonen KI-Kenntnisse haben müssen. Eine Beschränkung auf ausschließlich automatisierte Entscheidungen ist aber nicht vorgesehen. Außerdem bleibt das Grundproblem bestehen, dass es für die untersuchten Anwendungsszenarien grundsätzlich schwierig ist, solche KI-Systeme in ihrem Prozess zu unterbrechen.

[103] Kapitel 11 D. (S. 382).

Literaturverzeichnis

Abbou, Daniel, Schriftliche Stellungnahme für die am 26.09.2022 stattfindende Anhörung des Ausschusses für Digitales zur EU-Verordnung zu Künstlicher Intelligenz unter Einbeziehung Wettbewerbsfähigkeit im Bereich Künstliche Intelligenz und Blockchain-Technologie, 2022.

Abel, Ralf, Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO – Anwendungsbereich und Grenzen im nicht-öffentlichen Bereich, ZD 2018, S. 304-307.

Adesso, KI – eine Bestandsaufnahme, 2021.

Aichroth, Patrick/Battis, Verena/Dewes, Andreas u.a., Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens, 2020.

Ajunwa, Ifeoma, Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, SLU 2018, S. 21-53.

Alexy, Robert, Theorie der Grundrechte, Berlin, 1994.

Algorithm Watch, Draft AI Act: EU needs to live up to its own ambitions in terms of governance and enforcement, 2021.

Aligbe, Patrick, Einstellungs- und Eignungsuntersuchungen, 2. Aufl., München, 2021.

Allhutter, Doris/Cech, Florian/Fischer, Fabian/Grill, Gabriel/Mager, Astrid, Algorithmic Profiling of Job Seekers in Austria: How Austerity Politics Are Made Effective, Frontiers in big data, 2020.

Alpaydin, Ethem, Maschinelles Lernen, 3. Aufl., Berlin, 2022.

Andersson, Emilia/Sørvik, Gard Ove, Reality Lost? Re-Use of Qualitative Data in Classroom Video Studies, FQS 2013, S. 1-25.

Antonio Ginart/Melody Guan/Gregory Valiant/James Y. Zou, Making AI Forget You: Data Deletion in Machine Learning, NIPS'19: Proceedings of the 33rd International Conference on Neural Information Processing Systems 2019, S. 3518-3531.

Apel, Simon/Kaulartz, Markus, Rechtlicher Schutz von Machine Learning-Modellen, RDi 2020, S. 24-34.

Arbeit plus, Algorithmen und das AMS Arbeitsmarkt-Chancen-Modell – Zum Einsatz automatisierter Entscheidungs- und Profilingsysteme im arbeitsmarktpolitischen Bereich. Eine Positionierung von arbeit plus, 2019.

Arnold, Christian/Günther, Jens (Hrsg.), Arbeitsrecht 4.0 – Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt, 2. Aufl., München 2022 (zit. Arnold/Günther Arb. 4.0-Hdb/*Bearbeiter*).

Art. 29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260), 2018.

dies., Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259), 2018.

dies., Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251), 2018.

dies., Leitlinien zur DSFA und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248), 2017.

dies., Opinion 03/2013 on purpose limitation (WP 203) 2013.

dies., Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (WP 136).

dies., Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216), 2014.

Asgari, Nima, Datenschutz im Arbeitsverhältnis, DB 2017, S. 1325-1328.

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019 (zit. Auer-Reinsdorff/Conrad/*Bearbeiter*).

Bäcker, Rainer/Jansen, Kristina, Potenzialbeurteilung in einer digitalen Welt – Zwischen Persönlichkeitsverständnis und Mengenanalyse, in: Gourmelon, Andreas (Hrsg.), Personalauswahl – ein Blick in die Zukunft, Heidelberg, 2018.

Bahner, Elin, Übersteigertes Vertrauen in Automation: Der Einfluss von Fehlererfahrungen auf Complacency und Automation Bias, Berlin, 2008.

Bär, Tobias, Algorithmic Bias: Verzerrungen durch Algorithmen verstehen und verhindern – Ein Leitfaden für Entscheider und Data Scientists, Wiesbaden, 2022.

Barocas, Solon/Selbst, Andrew D., Big Data's Disparate Impact, Cal. L. Rev. 2016, S. 671-732.

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, Information Fusion 58 (2020), S. 82-115.

Bartke, Lukas/Hoffmann, Kira-Sophie/Skiebe, Daniel, Der Schutz von Trainingsdaten de lege ferenda – What would Machlup do?, RDi 2022, 431-439.

Bartsch, Alexander/Oerke, Sophie, Zum Grundsatz der Direkterhebung von Daten beim Betroffenen und dem nach Art. 4 Nr. 7 DS-GVO datenschutzrechtlich Verantwortlichen beim Handeln juristischer Personen, IR 2022, S. 155-156.

Basu, Jayanta Kumar/Bhattacharyya, Debnath/Tai-hoon, Kim, Use of Artificial Neural Network in Pattern Recognition, IJSEA 2010, S. 23-34.

Battis, Verena/Graner, Lukas, Risiken für die Privatheit aufgrund von Maschinellem Lernen, in: Reussner/Koziolek/Heinrich (Hrsg.), Informatik 2020, Lecture Notes in Informatics (LNI), Bonn 2021, S. 841-853.

Bauerschmidt, Jonathan, Grundsätze der europäischen Gesetzgebung, JuS 2022, S. 626-631.

Baumgartner, Renate, Künstliche Intelligenz in der Medizin: Diskriminierung oder Fairness?, in: Bauer, Gero/Kechaja, Maria u.a. (Hrsg.), Diskriminierung und Antidiskriminierung – Beiträge aus Wissenschaft und Praxis, Bielefeld 2021, S. 160-164.

Beck, Susanne, Künstliche Intelligenz – ethische und rechtliche Herausforderungen, in: Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, München, 2019.

dies., Künstliche Intelligenz und Diskriminierung: Herausforderungen und Lösungsansätze – Whitepaper aus der Plattform Lernende Systeme, Deutsche Nationalbibliothek, 2019.

dies./Kusche, Carsten/Valerius, Brian (Hrsg.), Digitalisierung, Automatisierung, KI und Recht – Festgabe zum 10-jährigen Bestehen der Forschungsstelle RobotRecht, Baden-Baden, 2020.

Beigang, Steffen/Fetz, Karolina/Kalkum, Dorina/Otto, Magdalena, Diskriminierungserfahrungen in Deutschland – Ergebnisse einer Repräsentativ- und einer Betroffenenbefragung, 2017.

Benecke, Martina, Das Verschulden des Arbeitgebers bei den Ansprüchen nach § 15 AGG, in: Brose, Wiebke/Greiner, Stefan u.a. (Hrsg.), Grundlagen des Arbeits- und Sozialrechts – Festschrift für Ulrich Preis zum 65. Geburtstag, München 2021, S. 73-83.

Berberich, Nicolas, Algorithmen, in: Kerstin, Kristian/Lampert, Christoph/Rothkopf, Constantin (Hrsg.), Wie Maschinen lernen – Künstliche Intelligenz verständlich erklärt, Heidelberg, 2019, S. 11-20.

Berendt, Bettina, The AI Act Proposal: Towards the next transparency fallacy?, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen, 2022, S. 31-53.

Bergt, Matthias, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, S. 365-371.

Betz, Christoph, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, S. 148-152.

Beyer, Elena/Erler, Katharina/Hartmann, Christoph/Kramme, Malte/Müller, Michael F./Pertot, Tereza/Tuna, Elif/Hilke Felix M. (Hrsg.), Privatrecht 2050 – Blick in die digitale Zukunft – Jahrbuch Junge Zivilrechtswissenschaft 2019, Baden-Baden, 2020.

Biewer, Sebastian/Baum, Kevin/Hermanns, Holger/Hetmank, Sven/Langer, Markus/Lauber-Rönsberg, Anne/Lehr, Franz/Sterz, Sarah, Software Doping Analysis for Human Oversight, S. 1-66.

Bissels, Alexander/Meyer-Michaelis, Isabel/Schiller, Jan, Arbeiten 4.0: Big Data-Analysen im Personalbereich, DB 2016, S. 3042-3049.

Bitkom, Woran scheitern Einstellungen?, 2018.

Bittner, Jürgen/Debowski, Nicole/Lorenz, Marco/Raber, Hans Georg/Steege, Hans/Teille, Karl, Recht und Ethik bei der Entwicklung von Künstlicher Intelligenz für die Mobilität, NZV 2021, S. 505-514.

Bleckat, Alexander, Anwendbarkeit der Datenschutzgrundverordnung auf künstliche Intelligenz, DuD 2020, S. 194-198.

Blinn, Nicole, Wearables und Arbeitnehmerdatenschutz – Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, DSRITB 2016, S. 519-534.

Block, Helga, 23. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 2017.

Blum, Benjamin, People Analytics, Baden-Baden, 2021.

Boenisch, Franziska, Privatsphäre und Maschinelles Lernen, DuD 2021, S. 448-452.

Bomhard, David/Merkle, Marieke, Europäische KI-Verordnung – Der aktuelle Kommissionsentwurf und praktische Auswirkungen, RDi 2021, S. 276-283.

dies., Der Entwurf eines EU Data Acts – Neue Spielregeln für die Data Economy, RDi 2022, S. 168-176.

Bomhard, David/Siglmüller, Jonas, Europäische KI-Haftungsrichtlinie – Der aktuelle Kommissionsentwurf und seine praktischen Auswirkungen, RDi 2022, S. 506-513.

Borgert, Stephanie/Helfritz, Kai H., Künstliche Intelligenz in HR – Eine Befragung der Deutschen Gesellschaft für Personalführung e.V., der TU Kaiserslautern und des Algorithm Accountability Lab, 2019.

Borges, Georg, IT und Software: Haftung für KI-Systeme, CR 2022, S. 553-561.

Braegelmann, Tom/Kaulartz, Markus (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020 (zit. Braegelmann/Kaulartz/*Bearbeiter*).

Braun, Sven, Vorherige Konsultation der Datenschutzaufsicht nach Folgenabschätzung – Analyse von Praxisempfehlungen zum derzeitigen Stand, ZD 2021, S. 297-302.

Braun Binder, Nadja/Spielkamp, Matthias/Egli, Catherine/Freiburghaus, Laurent/Kunz, Eliane/Laukenmann, Nina/Loi, Michele/Mätzener, Anna/Obrecht, Liliane/Wulf, Jessica, Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen, 2021.

Bretthauer, Sebastian, Intelligente Videoüberwachung, Baden-Baden, 2017.

ders., in: Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, München, 2019.

Breyer, Jonas, Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-GVO, DuD 2018, S. 311-317.

Brink, Stefan/Wolff, Heinrich Amadeus/v. Ungern-Sternberg, Antje (Hrsg.), BeckOK Datenschutzrecht, 45. Ed., München 2023 (zit. BeckOK Datenschutzrecht/*Bearbeiter*).

Brkan, Maja, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, Int J Law Info Tech 27 (2019), S. 91-121.

Brosius-Gersdorf, Frauke (Hrsg.), Dreier-Grundgesetz-Kommentar, 4. Aufl., Tübingen 2023 (zit. Dreier-Grundgesetz-Kommentar/*Bearbeiter*).

Bryson, Joanna/Haataja, Meeri, Reflections on the EU's AI Act and How We Could Make It Even Better, Competition Policy International 14.03.2022.

Büchner, Stefanie/Dosdall, Henrik, Organisation und Algorithmus – Wie algorithmische Kategorien, Vergleiche und Bewertungen durch Organisationen relevant gemacht werden, KZfSS 2021, S. 333-357.

Buhl, Samir/Frieling, Tino/Krois, Christopher/Malorny, Friederike/Münder, Matthias/Richter, Barbara/Schmidt, Laura (Hrsg.), Der erwachte Gesetzgeber – Regulierung und Deregulierung im Arbeitsrecht: Dokumentation der 7. Assistentinnen- und Assistententagung im Arbeitsrecht vom 27.-29.07.2017, Baden-Baden, 2017.

Bundesregierung, Strategie Künstliche Intelligenz der Bundesregierung, 2018.

Bundesverband der Personalmanager, Zwischen Euphorie und Skepsis – KI in der Personalarbeit, 2019.

Bunnenberg, Jan Niklas, Privatautonomie und Datenschutz – Zum Verhältnis privater und staatlicher Regelbildung im Recht der Verbraucherdatenverarbeitung, JZ 2020, S. 1088-1097.

ders., Privates Datenschutzrecht, Baden-Baden, 2020.

Burchardi, Sophie, Risikotragung für KI-Systeme – Zur Zweckmäßigkeit einer europäischen Betreiberhaftung, EuZW 2022, S. 685-692.

Burrell, Jenna, How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society 3 (2016), S. 1-12.

Bussche, Axel von dem, Anmerkung zu LG Bonn, Urteil v. 11.11.2020 – 29 OWi 1/20, ZD 2021, S. 154-161.

ders./Voigt, Paul (Hrsg.), Konzerndatenschutz, 2. Aufl., München 2019 (zit. von dem Bussche/Voigt/*Bearbeiter*).

Buxmann, Peter/Schmidt, Holger, Künstliche Intelligenz – Mit Algorithmen zum wirtschaftlichen Erfolg, 2018.

BVMed-Positionen zum Entwurf des „Artificial Intelligence Act" (AIA), MPR 2021, S. 176-182.

Byers, Philipp/Fischer, Christian, Rechtliche Vorgaben bei der Durchführung von sog. „Backgroundchecks", ArbRAktuell 2022, S. 90-93.

Calliess, Christina/Ruffert, Matthias (Hrsg.), EUV/AEUV, 6. Aufl., München 2022 (zit. Calliess/Ruffert/*Bearbeiter*).

Cheng, Maggie M./Hackett, Rick D., A critical review of algorithms in HRM: Definition, theory, and practice, Human Resource Management Review 31 (2021), S. 1-14.

Chiba, Stefanie, Sind vollautomatisierte positive Entscheidungen unter Art. 22 DSGVO zu subsumieren?, Dako 2020, S. 85-87.

Coester, Ulla, Vertrauenswürdige KI – zwischen Anspruch und Wirklichkeit, DuD 2020, S. 245-249.

Conrad, Conrad, DSGVO 2.0 – Effizienter(er) Schutz durch KI?, DSRITB 2019, S. 391-409.

Culik, Nicolai/Döpke, Christian, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, S. 226-230.

ders., Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, 2018.

Cynthia C. S. Liem/Markus Langer/Andrew M Demetriou/Annemarie M. F. Hiemstra/Cornelius J. König, Psychology Meets Machine Learning: Interdisciplinary Perspectives on Algorithmic Job Candidate Screening, in: Escalante, Hugo Jair./Escalera, Sergio. u.a. (Hrsg.), Explainable and Interpretable Models in Computer Vision and Machine Learning, Cham 2018, S. 197-253.

Dallmann, Michael/Busse, Philipp, Verarbeitung von öffentlich zugänglichen personenbezogenen Daten – Datenschutzrechtliche Voraussetzungen und Grenzen, ZD 2019, S. 394-399.

Datenethikkommission, Gutachten der Datenethikkommission, 2019.

Datenschutzbehörde Österreich, DSB Bescheid v. 16.8.2020, DSB-D213.2020 2020-0-513.605 – Arbeitsmarktchance Assistenz-System (AMAS), ZIIR 2020, 410-416.

Datenschutzkonferenz (DSK), Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen, 2018.

dies., Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, 2019.

dies., Kurzpapier Nr. 13 – Auftragsverarbeitung, Art. 28 DS-GVO, 2018.

dies., Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 2018.

dies., Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 2019.

Däubler, Wolfgang, Gläserne Belegschaften – Das Handbuch zum Beschäftigtendatenschutz, 9. Aufl., Frankfurt am Main, 2021.

ders., Informationsbedarf versus Persönlichkeitsschutz – was muss, was darf der Arbeitgeber wissen?, NZA 2017, S. 1481-1488.

ders./Beck, Thorsten (Hrsg.), Allgemeines Gleichbehandlungsgesetz, 5. Aufl., Baden-Baden, 2022 (zit. Däubler/Beck/*Bearbeiter*).

ders./Hjort Jens Peter/Schubert, Michael/Wolmerath Martin (Hrsg.), Arbeitsrecht – Individualarbeitsrecht mit kollektivrechtlichen Bezügen, 5. Aufl., Baden-Baden 2022 (zit. HK-ArbR/*Bearbeiter*).

Dauth, Georg, Führen mit dem DISG-Persönlichkeitsprofil, 2012.

Der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit (BfDI), Positionspapier zur Anonymisierung unter der DSGVO unter Berücksichtigung der TK-Branche, 2020.

Der Europäische Datenschutzausschuss (EDSA), Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default 2020.

ders., Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 2020.

Djeffal, Christian, Art. 22 DSGVO als sozio-technische Gestaltungsnorm, DuD 2021, S. 529-533.

Döbel, Inga/Leis, Miriam/Vogelsang, Manuel Malina/Neustroev, Dmitry/Petzka, Henning/Riemer, Annamaria/Rüping, Stefan/Voss, Angelika/Wegele, Martin/Wetz, Juliane, Maschinelles Lernen – Eine Analyse zu Kompetenzen, Forschung und Anwendung, 2018.

Dörr, Oliver/Grote, Rainer, Marauhn, Thilo (Hrsg.), EMRK/GG – Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, 3. Aufl., Tübingen, 2022 (zit. Dörr/Grote/Marauhn/*Bearbeiter*).

Dovas, Maria-Urania, Die Datenschutzfolgenabschätzung in der DSGVO, ITRB 2019, S. 14-20.

Drechsler, Jörg/Jentsch, Nicola, Synthetische Daten – Innovationspotential und gesellschaftliche Herausforderungen, 2018.

Dreyer, Stephan, Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, S. 135-144.

ders./Schulz, Wolfgang, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, 2018.

Düwell, Franz Josef/Brink, Stefan, Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung: Viele Änderungen und wenig Neues, NZA 2017, S. 1081-1085.

Dzida, Boris, Big Data und Arbeitsrecht, NZA 2017, S. 541-546.

ders., Neue datenschutzrechtliche Herausforderungen für das Personalmanagement, BB 2019, S. 3060-3067.

ders./Grau, Timon, Beschäftigtendatenschutz nach der Datenschutzgrundverordnung und dem neuen BDSG, DB 2018, S. 189-194.

ders./Groh, Naemi, Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren, NJW 2018, S. 1917-1922.

dies., People Analytics im Personalbereich, ArbRB 2018, S. 179-182.

Ebers, Martin, Regulating Explainable AI in the European Union. An Overview of the Current Legal Framework(s), in: Colonna, Liane/Greenstein, Stanley (Hrsg.), Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence, 2022, S. 103-132.

ders./Heinze, Christian/Krügel, Tina/Steinrötter, Björn (Hrsg.), Künstliche Intelligenz und Robotik, 2020.

ders./Hoch, Veronica/Rosenkranz, Frank/Ruschemeier, Hannah/Steinrötter, Björn, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf – Eine kritische Bewertung durch Mitglieder der Robotics & AI Law Society (RAILS), RDi 2021, S. 528-537.

Ebert, Andreas/Spiecker gen. Döhmann, Indra, Der Kommissionsentwurf für eine KI-Verordnung der EU – Die EU als Trendsetter weltweiter KI-Regulierung, NVwZ 2021, S. 1188-1193.

Ebner, Gordian Konstantin, Weniger ist Mehr?, Baden-Baden, 2022.

Ehinger, Patrick/Stiemerling, Oliver, Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen, CR 2018, S. 761-770.

Ehmann, Eugen/Selmayr, Martin/Albrecht, Jan Philipp/Baumgartner, Ulrich/Bertermann, Nikolaus (Hrsg.), DS-GVO – Datenschutz-Grundverordnung, 2. Aufl., München/Wien, 2018 (zit. Ehmann/Selmayr/*Bearbeiter*).

Eichelberger, Jan, Der Vorschlag einer „Richtlinie über KI-Haftung", DB 2022, S. 2783-2789.

Eickstädt, Elina/Weaver, Calum Neil, Praktische Herausforderungen im Umgang mit datenschutzrechtlichen Betroffenenrechten – Lösungsansätze aus rechtlicher und informationstechnischer Sicht, DSRITB 2020, S. 287-304.

Electronic Privacy Information Center, Liberty at Risk: Pre-trial Risk Assessment Tools in the U.S., 2020.

Elter, Sven, Künstliche Intelligenz und kreative Erzeugnisse. Schutz von KI-geschaffenen Erzeugnissen, in: Beck, Susanne/Kusche, Carsten/Valerius, Brian (Hrsg.), Digitalisierung, Automatisierung, KI und Recht – Festgabe zum 10-jährigen Bestehen der Forschungsstelle RobotRecht, Baden-Baden, 2020, S. 181-197.

Engeler, Malte, Das überschätzte Koppelungsverbot – Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen, ZD 2018, S. 55-62.

EP-LIBE-Ausschuss, Änderungsanträge (5), AM – PE506.164v01-00.

Epping, Volker/Hillgruber, Christian (Hrsg.), BeckOK Grundgesetz, 56. Ed., München, 2023 (zit. BeckOK GG/*Bearbeiter*).

Ernst, Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, S. 1026-1036.

ders., Die Gefährdung der individuellen Selbstentfaltung durch den privaten Einsatz von Algorithmen, in: *Klafki, Anika/Würkert, Felix/Winter, Tina* (Hrsg.), Digitalisierung und Recht – Tagung des eingetragenen Vereins Junge Wissenschaft im öffentlichen Recht an der Bucerius Law School am 26. November 2016, Hamburg, 2017, S. 63-77.

Ernst, Stefan, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, S. 110-114.

ders., Verbraucherschutz durch „faire" Algorithmen – eine Illusion, VuR 2019, S. 401-403.

Ertel, Wolfgang, Grundkurs Künstliche Intelligenz, 5. Aufl., Wiesbaden, 2021.

Eschholz, Stefanie, Big Data-Scoring unter dem Einfluss der Datenschutz-Grundverordnung, DuD 2017, S. 180-185.

Europäische Kommission, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik im Hinblick auf Sicherheit und Haftung, 2020.

dies., Weißbuch – Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, 2020.

European Union Agency for Fundamental Rights, Bias in algorithms – Artificial intelligence and discrimination, 08.12.2022.

Feuerstack, Daniel, Menschenrechtliche Vorgaben an die Transparenz KI-basierter Entscheidungen und deren Berücksichtigung in bestehenden Regulierungsansätzen, Ordnung der Wissenschaft 2022, S. 167-180.

Fischer, Lorenz Lloyd, Die Horizontalwirkung der EU-Grundrechtecharta im Arbeitsrecht – Zulässigkeit und Grenzen der unionsgrundrechtlichen Effektuierung arbeitsrechtlicher Richtlinien, Tübingen, 2023.

Flink, Maike, Beschäftigtendatenschutz als Aufgabe des Betriebsrats, Berlin, 2020.

Folkerts, Elena, Wirklich freiwillig?, DuD 2022, S. 77-80.

Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz: Rechtshandbuch, 3. Aufl., München 2019 (zit. Forgó/Helfrich/Schneider/*Bearbeiter*).

Frank, Justus/Heine, Maurice, Künstliche Intelligenz im Betriebsverfassungsrecht, NZA 2021, S. 1448-1452.

Franzen, Martin, Das Verhältnis des Auskunftsanspruchs nach DS-GVO zu personalaktenrechtlichen Einsichtsrechten nach dem BetrVG, NZA 2020, S. 1593-1597.

ders., Datenschutz-Grundverordnung und Arbeitsrecht, EuZA 2017, S. 313-351.

ders., Persönlichkeitsrecht und Datenschutz im Arbeitsrecht, ZfA 2019, S. 18-39.

ders., Beschäftigtendatenschutz aus Luxemburg?, EuZA 2022, S. 261-262.

ders./Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 4. Aufl., München 2022 (zit. EuArbRK/*Bearbeiter*).

Freyler, Carmen, Robot-Recruiting, Künstliche Intelligenz und das Antidiskriminierungsrecht, NZA 2020, S. 284-290.

Friedewald, Michael/Schiering, Ina/Martin, Nicholas, Datenschutz-Folgenabschätzung in der Praxis, DuD 2019, S. 473-477.

Friedman, Batya/Nissenbaum, Helen, Bias in Computer Systems, ACM Transactions on Information Systems 1996, S. 330-347.

Gärtner, Christian, Smart HRM – Digitale Tools für die Personalarbeit, 2020.

Gausling, Tina, Künstliche Intelligenz und DSGVO, DSRITB 2018, S. 519-543.

dies., Künstliche Intelligenz im digitalen Marketing – Datenschutzrechtliche Bewertung KI-gestützter Kommunikations-Tools und Profiling-Maßnahmen, ZD 2019, S. 335-341.

dies., KI und DS-GVO im Spannungsverhältnis, in: Ballestrem, Johannes Graf/Bär, Ulrike u.a. (Hrsg.), Künstliche Intelligenz – Rechtsgrundlagen und Strategien aus der Praxis, Wiesbaden 2020, S. 11-50.

Geminn, Christian, Die Regulierung Künstlicher Intelligenz – Anmerkungen zum Entwurf eines Artificial Intelligence Act, ZD 2021, S. 354-359.

Gerhartl, Andreas, Betrachtungen zum AMAS-Algorithmus, ZIIR 2021, S. 24-29.

Gesellschaft für Informatik, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren – Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, 2018.

Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus (Hrsg.), EUV/AEUV, 7. Aufl., München 2023 (zit. Geiger/Khan/Kotzur/*Bearbeiter*).

Gerards, Janneke/Xenidis, Raphaele, Algorithmic discrimination in Europe – Challenges and opportunities for gender equality and non-discrimination law, 2021.

Gertz, Michael/Aumiller, Dennis, Legal Tech und Deep Learning – Eine Bestandsaufnahme, LTZ 2022.

Gierschmann, Sibylle, Gestaltungsmöglichkeiten durch systematisches und risikobasiertes Vorgehen – Was ist anonym? – Planung und Bewertung der Risiken der Anonymisierung, ZD 2021, S. 482-486.

Gigerenzer, Gerd, Das Schreckgespenst der digitalen Verhaltenssteuerung geht um, OBJEKT spektrum 2016, S. 6-7.

Glatzner, Florian, Profilbildung und algorithmenbasierte Entscheidungen, DuD 2020, S. 312-315.

Gless, Sabine/Janal, Ruth, in: Hilgendorf, Eric/Roth-Isigkeit, David (Hrsg.), Die neue Verordnung der EU zur künstlichen Intelligenz, München, 2023.

Glocker, Felix/Hoffmann, Maren, Beschäftigtendatenschutz: Zentrale Rechtsgrundlage nicht mehr anwendbar, BB 2023, S. 1333-1335.

Gola, Peter, Aus den aktuellen Berichten der Aufsichtsbehörden (33): Die Digitalisierung des Bewerbermanagements – Videointerviews bei der Bewerbung, RDV 2018, S. 24-28.

ders., Das Internet als Quelle von Bewerberdaten, NZA 2019, S. 654-658.

ders./Heckmann, Dirk (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl., München 2022 (zit. Gola/Heckmann/*Bearbeiter*).

Golland, Alexander, Der räumliche Anwendungsbereich der DS-GVO, DuD 2018, S. 351-357.

Gössl, Susanne Lilian, KI-Systeme und Diskriminierung – Eine Einführung, in: Diskriminierungsfreie KI, Bonn, 2023.

Götz, Thomas, Big Data im Personalmanagement – Datenschutzrecht und betriebliche Mitbestimmung, Baden-Baden, 2020.

Granetzny, Thomas, in: Thüsing, Gregor (Hrsg.), Beschäftigtendatenschutz und Compliance: effektive Compliance im Spannungsfeld von DS-GVO, BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 3. Aufl., München, 2021 (zit. Thüsing/Granetzny, Beschäftigtendatenschutz).

Greb, Christian/Linnenbürger, Anja, Einsatz von künstlicher Intelligenz und Sprachanalysetechnologien in der Personalauswahl, in: Gourmelon, Andreas (Hrsg.), Personalauswahl – ein Blick in die Zukunft, Heidelberg 2018, S. 75-85.

Grimm, Detlef/Singraven, Jonas, Digitalisierung und Arbeitsrecht – Personalarbeit 4.0: Gestaltung: Best Practices, Köln/Berlin 2022.

Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.), Europäisches Unionsrecht, 7. Aufl. 2015 (zit. von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht/*Bearbeiter*).

Grünberger, Michael, Reformbedarf im AGG: Beweislastverteilung beim Einsatz von KI, ZRP 2021, S. 232-235.

Grützmacher, Malte, Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO, CR 2021, S. 433-444.

Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan (Hrsg.), beck-online.GROSSKOMMENTAR 2023, Stand 01.09.2023 (zit. BeckOGK/*Bearbeiter*).

Gumpp, Tobias, Stellenwert der Erwägungsgründe in der Methodenlehre des Unionsrechts, ZfPW 2022, S. 446-476.

Günther, Jens/Böglmüller, Matthias, Künstliche Intelligenz und Roboter in der Arbeitswelt, BB 2017, S. 53-58.

Günther-Burmeister, Jan-Philipp, Europäische Verordnungsentwürfe zur Regulierung Künstlicher Intelligenz, DB 2021, S. 1858-1862.

Guo, Qi/Geyik, Sahin Cem/Ozcaglar, Cagri/Thakkar, Ketan/Anjum, Nadeem/Kenthapadi, Krishnaram, The AI Behind LinkedIn Recruiter search and recommendation systems, https://perma.cc/4MHV-U67E.

Haataja, Meeri/Bryson, Joanna J., The European Parliament's AI Regulation, AC 4 (2023), S. 707-718.

Hacker, *Philipp*, Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, S. 148-197.

ders., Stellungnahme für die Öffentliche Anhörung „Generative Künstliche Intelligenz" am Mittwoch, 24. Mai 2023, 14:30 – 16:30 Uhr, Sitzungssaal Reichstagsgebäude (RTG) 3 N 001.

ders., Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law, CMLR 2018, S. 1143-1186.

ders., Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz, RW 2018, S. 243-288.

ders., Datenprivatrecht – Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB, Tübingen, 2020.

ders., Ein Rechtsrahmen für KI-Trainingsdaten, ZGE 2020, S. 240-270.

ders., Europäische und nationale Regulierung von Künstlicher Intelligenz, NJW 2020, S. 2142-2147.

ders., A legal framework for AI training data—from first principles to the Artificial Intelligence Act, Law, Innovation and Technology 13 (2021), S. 257-301.

ders./Wessel, Lauri, KI-Trainingsdaten nach dem Verordnungsentwurf für Künstliche Intelligenz, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen, 2022.

Hähnchen, Susanne/Schader, Paul/Weiler, Frank/Wischmeyer, Thomas, Legal Tech – Rechtsanwendung durch Menschen als Auslaufmodell?, JuS 2020, S. 625-635.

Härting, Niko, Zweckbindung und Zweckänderung im Datenschutzrecht, NJW 2015, 3284-3288.

Hartmann, Frank/Kriebel, Lennart, Art. 22 DSGVO, Art. 1 GRCH und HAL 9000, DSRITB 2021, S. 129-148.

Hau, Wolfgang/Poseck, Roman (Hrsg.), BeckOK BGB, 67. Aufl., München, 2022 (zit. BeckOK BGB/*Bearbeiter*).

Hauer, Marc/Raudonat, Franziska/Zweig, Katharina, Anwendungsszenarien: KI-Systeme im Personal- und Talentmanagement, 2020.

Havlíková, Štěpánka, Automatisierte Sprachanalysen – ihr Einsatz in Personalwesen, bei der Kundenbetreuung oder im Gesundheitswesen, DSRITB 2020, S. 141-159.

Heesen, Jessica/Reinhardt, Karoline/Schelenz, Laura, Diskriminierung durch Algorithmen vermeiden: Analysen und Instrumente für eine demokratische digitale Gesellschaft, in: Bauer, Gero/Kechaja, Maria u.a. (Hrsg.), Diskriminierung und Antidiskriminierung – Beiträge aus Wissenschaft und Praxis, Bielefeld, 2021.

Heil, Maria, Regulatorische Herausforderungen für KI-basierte Medizinprodukte-Software, MPR 2022, S. 1-12.

Heine, Maurice, Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis – Zum Einsatz „Künstlicher Intelligenz" in arbeitsrechtlichen Entscheidungsprozessen, Berlin, 2023.

Heinrich, Bernd/Klier, Matthias, Datenqualitätsmetriken für ein ökonomisch orientiertes Qualitätsmanagement, in: *Hildebrand, Knut/Gebauer, Marcus/Mielke, Michael* (Hrsg.), Daten- und Informationsqualität: die Grundlage der Digitalisierung, 5. Aufl., Wiesbaden, 2021.

Herberger, Marie, Verbandsklageverfahren für diskriminierungsrechtliche Ansprüche, RdA 2022, S. 220-228.

Herder, Janosik, Regieren Algorithmen? Über den sanften Einfluss algorithmischer Modelle, in: Kar, Resa Mohabbat/Thapa, Basanta/Parycek, Peter (Hrsg.), (Un)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2018.

Herfurth, Constantin, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, ZD 2018, S. 514-520.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung, Baden-Baden, 2016.

Hilgers, Hans Anton, Aktuelle Änderungen im BDSG – Weitere Öffnung der Verarbeitung sensibler Daten für nicht-öffentliche Stellen, ZD 2020, S. 556-561.

Hitzelberger-Kijima, Yukiko, Die Einwilligung von Beschäftigten in die Verarbeitung ihrer personenbezogenen Daten durch den Arbeitgeber, öAT 2020, S. 133-136.

Hoeren, Thomas/Niehoff, Maurice, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, RW 2018, S. 47-66.

ders./Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, 58. EL, München 2022 (zit. Hoeren/Sieber/Holznagel, MultimediaR-Hdb/*Bearbeiter*).

Hoffmann, Michel, Möglichkeit und Zulässigkeit von Künstlicher Intelligenz und Algorithmen im Recruiting, NZA 2022, S. 19-24.

Hoffmann-Riem, Wolfgang, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), S. 1-42.

ders., Die digitale Transformation als Herausforderung für die Legitimation rechtlicher Entscheidungen, in: Unger, Sebastian/Ungern-Sternberg, Antje von (Hrsg.), Demokratie und künstliche Intelligenz, Tübingen, 2019.

Hofmann, Kai, „Smart Factory" – Arbeitnehmerdatenschutz in der Industrie 4.0, DSRITB, S. 209-224.

Holl, Jürgen/Kernbeiß, Günter/Wagner-Pinter, Michael, Das AMS-Arbeitsmarktchancen-Modell, 2018.

Holthausen, Joachim, Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, RdA 2021, S. 19-32.

Hölzel, Julian, Anonymisierungstechniken und das Datenschutzrecht, DuD 2018, S. 502-509.

Holzinger, Andreas/Goebel, Randy/Fong, Ruth/Moon, Taesup/Müller, Klaus-Robert/Samek, Wojciech (Hrsg.), xxAI - Beyond Explainable AI – International Workshop Held in Conjunction with ICML 2020 July 18, 2020, Vienna, Austria, Revised and Extended Papers, 2022.

Holzinger, Andreas/Saranti, Anna/Molnar, Christoph/Biecek, Przemyslaw/Samek, Wojciech, Explainable AI Methods – A Brief Overview, in: Holzinger, Andreas/Goebel, Randy u.a. (Hrsg.), xxAI - Beyond Explainable AI – International Workshop Held in Conjunction with ICML 2020 July 18, 2020, Vienna, Austria, Revised and Extended Papers, 2022, S. 13-38.

Höpfner, Clemens/Daum, Jan Alexander, Der „Robo-Boss" – Künstliche Intelligenz im Arbeitsverhältnis, ZfA 2021, S. 467-501.

Hoppe, Florian, Technische Grundlagen, in: Hartmann, Matthias (Hrsg.), KI & Recht kompakt, 2020, S. 1-28.

Hornung, Gerrit, KI-Regulierung im Mehrebenensystem, DuD 2022, S. 561-566.

ders., Trainingsdaten und die Rechte von betroffenen Personen, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen 2022, S. 91-121.

ders./Wagner, Bernd, Anonymisierung als datenschutzrechtliche Verarbeitung? – Rechtliche Anforderungen und Grenzen für die Anonymisierung personenbezogener Daten, ZD 2020, S. 223-228.

Huang, He-Ming/Xiao, Yu/Yang, Rui/Yu, Ye-Tian/He, Hui-Kai/Whang, Zhe/Guo, Xin, Implementation of Dropout Neuronal Units Based on Stochastic Memristive Devices in Neural Networks with High Classification Accuracy, Adv. Sci. 2020,7, 2001842.

Hütt, Marc-Thorsten/Schubert, Claudia, Fairness von KI-Algorithmen, in: Mainzer, Klaus (Hrsg.), Philosophisches Handbuch Künstliche Intelligenz, 2020.

Imping, Andreas, Digitalisierung im Personalbereich: Rechtliche Rahmenbedingungen und Gestaltungsoptionen bei Betriebsvereinbarungen, DB 2021, S. 1808-1818.

Jacob, Leon/Kyaw, Felicitas von, Mitarbeiterorientierung als Wettbewerbsvorteil – Mit Employee Experience Design mitarbeiterorientierte Personalarbeit gestalten, in: Gärtner, Christian (Hrsg.), Smart Human Resource Management – Analytics, Automatisierung udn Agilität in der Personalarbeit, Wiesbaden 2020, S. 53-80.

Janal, Ruth, Konfliktlinien: Geheimhaltungsinteressen vs. Transparenz, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen, 2022, S. 123-141.

Jandt, Silke/Steidle, Roland (Hrsg.), Datenschutz im Internet, Baden-Baden 2018 (zit. Jandt/Steidle/*Bearbeiter*).

Jarass, Hans/Kment, Martin (Hrsg.), Grundgesetz für die Bundesrepublik Deutschland: Kommentar, 17. Aufl., München, 2022 (zit. Jarass/Pieroth/*Bearbeiter*).

Jares, Patricia/Vogt, Tobias, Der Einsatz von KI-basierter Sprachanalyse im Bewerbungsverfahren, in: Knappertsbusch, Inka/Gondlach, Kai (Hrsg.), Arbeitswelt und KI 2030 – Herausforderungen und Strategien für die Arbeit von morgen, Wiesbaden, 2021.

Jebur, Ameer/Al-Jumeily, Dhiya/Aljanabi, Khalid/Al Khaddar, Rafid/Atherton, William/Alattar, Zeinab/Majeed, Adel/Mustafina, Jamila, New Applications of a Supervised Computational Intelligence (CI) Approach: Case Study in Civil Engineering, in: Berry, Michael W./Mohamed, Azlinah/Yap, Bee Wah (Hrsg.), Supervised and Unsupervised Learning for Data Science, 2020, S. 145-182.

Joos, Daniel, Einsatz von künstlicher Intelligenz im Personalwesen unter Beachtung der DS-GVO und des BDSG, NZA 2020, S. 1216-1221.

ders./Meding, Kristofer, Künstliche Intelligenz und Datenschutz im Human Resource Management, CR 2020, S. 834-840.

Jüngling, Alexander, Die Digitalstrategie der EU-Kommission: Regulierung von Künstlicher Intelligenz, MMR 2020, S. 440-445.

Käde, Lisa/Maltzan, Stephanie von, Die Erklärbarkeit von Künstlicher Intelligenz (KI) – Entmystifizierung der Black Box und Chancen für das Recht, CR 2020, S. 66-72.

Kainer, Friedemann/Weber, Christian, Datenschutzrechtliche Aspekte des „Talentmanagements", BB 2017, S. 2740-2747.

Kalogeropoulos, Elena/Lammers, Anne/Brehm-Müller, Jaana/Puntschuh, Michael, Wegweiser Digitale Debatten – Teil 1: Algorithmische Systeme, S. 1-15.

Kämmerer, Jörn A./Kotzur, Markus von (Hrsg.), Grundgesetz-Kommentar, 7. Aufl., München, 2021 (zit. von Münch/Kunig/*Bearbeiter*).

Karaarduc, Melda, Zur Frage der systematischen Diskriminierung durch das Arbeitsmarktchancen-Assistenz-System, EALR 2021, S. 35-44.

Kersting, Miriam, Moderner Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu?, in: *Buhl, Samir/Frieling, Tino* u.a. (Hrsg.), Der erwachte Gesetzgeber – Regulierung und Deregulierung im Arbeitsrecht: Dokumentation der 7. Assistentinnen- und Assistententagung im Arbeitsrecht vom 27.-29.07.2017, Baden-Baden, 2017, S. 55-75.

Keßler, Oliver, Intelligente Roboter - neue Technologien im Einsatz, MMR 2017, S. 589-594.

Klar, Manuel, Künstliche Intelligenz und Big Data – algorithmenbasierte Systeme und Datenschutz im Geschäft mit Kunden, BB 2019, S. 2243-2252.

Klösel, Daniel/Mahnhold, Thilo, Die Zukunft der datenschutzrechtlichen Betriebsvereinbarung – Mindestanforderungen und betriebliche Ermessensspielräume nach DS-GVO und BDSG nF, NZA 2017, S. 1428-1433.

Knitter, Philipp, Digitale Weisungen, Berlin, 2022.

Knobloch, Tobias/Hustedt, Carla, Der maschinelle Weg zum passenden Personal – Zur Rolle algorithmischer Systeme in der Personalauswahl, 2019.

Knuchel, Christian/Ebert, Nico, DSGVO-konformes Löschen, DuD 2020, S. 126-127.

Kohne, Andreas/Kleinmanns Philipp/Rolf, Christian/Beck, Moritz, Chatbots – Aufbau und Anwendungsmöglichkeiten von autonomen Sprachassistenten, Wiesbaden, 2020.

Köhnlechner, Daniela, Auskunftsrecht des Betroffenen nach der Datenschutz-Grundverordnung (DSGVO), DSRITB 2018, S. 173-181.

Kolain, Michael/Grafenauer, Christian/Ebers, Martin, Anonymity Assessment – A Universal Tool for Measuring Anonymity of Data Sets Under the GDPR with a Special Focus on Smart Robotics, 2021.

Köllmann, Thomas, Implementierung elektronischer Überwachungseinrichtungen durch Betriebsvereinbarung vor dem Hintergrund der DSGVO, Baden-Baden 2021.

Kollmar, Frederike/El-Auwad, Maya, Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, DSRITB 2020, S. 199-213.

Konertz, Roman/Schönhof, Raoul, Das technische Phänomen „Künstliche Intelligenz" im allgemeinen Zivilrecht – Eine kritische Betrachtung im Lichte von Autonomie, Determinismus und Vorhersehbarkeit, Baden-Baden, 2020.

Kopp, Reinhold/Sokoll, Karen, Wearables am Arbeitsplatz – Einfallstore für Alltagsüberwachung?, NZA 2015, S. 1352-1358.

Korch, Stefan/Chatard, Yannick, Der Missbrauchseinwand gegen Betroffenenrechte – Eine Standortbestimmung zum Umgang mit datenschutzfremden Motiven, ZD 2022, S. 482-486.

Körner, Marita, Die Datenschutz-Grundverordnung und nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz, NZA 2016, S. 1383-1386.

dies., Beschäftigtendatenschutz in Betriebsvereinbarungen unter Geltung der DS-GVO, NZA 2019, S. 1389-1395.

dies., Drei Jahre Beschäftigtendatenschutz unter der Datenschutzgrundverordnung, NZA 2021, S. 1137-1143.

Kort, Michael, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, S. 711-716.

ders., Die Bedeutung der neueren arbeitsrechtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes, NZA 2018, S. 1097-1105.

Kossen, Jannik/Kuruc, Fabrizio/Müller, Maike Elisa, Einleitung, in: Kerstin, Kristian/Lampert, Christoph/Rothkopf, Constantin (Hrsg.), Wie Maschinen lernen – Künstliche Intelligenz verständlich erklärt, Heidelberg 2019, S. 3-10.

Kiel, Heinrich/Lunk, Stefan/Oetker, Hartmut (Hrsg.), Münchener Handbuch zum Arbeitsrecht – Band 1: Individualarbeitsrecht I, 5. Aufl., München 2021 (zit. MHdb ArbR Band 1/*Bearbeiter*).

Krafft, Tobias/Zweig, Katharina, Wie Gesellschaft algorithmischen Entscheidungen auf den Zahn fühlen kann, in: Kar, Resa Mohabbat/Thapa, Basanta/Parycek, Peter (Hrsg.), (Un)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2018.

dies., Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse – Ein Regulierungsvorschlag aus sozioinformatischer Perspektive, 2019.

Kramer, Stefan (Hrsg.), IT-Arbeitsrecht – Digitalisierte Unternehmen: Herausforderungen und Lösungen, München 2019 (zit. *Bearbeiter*, in: Kramer (Hrsg.), Kramer IT-ArbR).

Kraus, Tom/Ganschow, Lena/Eisenträger, Marlene/Wischmann, Steffen, Erklärbare KI, 2021.

Krause, Rüdiger, Digitalisierung der Arbeitswelt - Herausforderungen und Regelungsbedarf – Gutachten B zum 71. Deutschen Juristentag, München, 2016.

ders., Arbeitsmarktchancen per Algorithmus?, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen 2022, S. 143-163.

Kreutzer, Till/Christiansen, Per, KI in Unternehmen – Ein Praxisleitfaden zu rechtlichen Fragestellungen, 2021.

Kring, Markus/Marosi, Johannes, Ein Elefant im Porzellanladen - Der EuGH zu Personenbezug und berechtigtem Interesse, K&R 2016, S. 773-776.

Kroll, Joshua/Huey, Joanna/Barocas, Solon/Felten, Edward/Reidenberg, Joel/Robinson, David/Yu, Harlan, Accountable Algorithms, Univ. Pa. Law Rev. 165 (2017), S. 633.

Krüger, Julia/Lischka, Konrad, Damit Maschinen den Menschen dienen können – Lösungsansätze, um algorithmische Prozesse in den Dienst der Gesellschaft zu stellen, 2018.

dies., Was zu tun ist, damit Maschinen den Menschen dienen, in: Kar, Resa Mohabbat/Thapa, Basanta/Parycek, Peter (Hrsg.), (Un)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2018.

Krusche, Jan, Kumulation von Rechtsgrundlagen zur Datenverarbeitung – Verhältnis der Einwilligung zu anderen Erlaubnistatbeständen, ZD 2020, S. 232-237.

Kühling, Jürgen, Das „Recht auf Vergessenwerden" vor dem BVerfG – November-(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, NJW 2020, S. 275-280.

ders./Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung – BDSG, 3. Aufl., München, 2020 (zit. Kühling/Buchner/*Bearbeiter*).

ders./Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW, S. 448-454.

Kullmann, Miriam, Diskriminierung durch algorithmische Entscheidungen: „Equality Through Algorithmic Design", in: Beyer, Elena/Erler, Katharina u.a. (Hrsg.), Privatrecht 2050 – Blick in die digitale Zukunft – Jahrbuch Junge Zivilrechtswissenschaft 2019, Baden-Baden, 2020, S. 227-254.

Kumar, Senthil, Data Mining Based Marketing Decision Support System Using a Hybrid Machine Learning Algorithm, Journal of Artificial Intelligence and Capsule Networks, 2020, S. 185-193.

Kumkar, Lea Katharina/Roth-Isigkeit, David, Erklärungspflichten bei automatisierten Datenverarbeitungen nach der DSGVO, JZ 2020, 277-286.

Kuntz, Thilo, Künstliche Intelligenz, Wissenszurechnung und Wissensverantwortung, ZfPW 2022, S. 178-206.

Kuschel, Linda/Asmussen, Sven/Golla, Sebastian J. (Hrsg.), Intelligente Systeme – intelligentes Recht – GRUR Junge Wissenschaft Hamburg 2020/2021, Baden-Baden 2021.

Kuß, Christian, G. Beschäftigtendatenschutz, in: Kuß, Christian/Steege, Hans/Chibanguza, Kuuya Josef (Hrsg.), Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden, 2022.

Landge, Maheshkumar B./Mahajan, Deepali/Mahender, C. Namrata, Correlating Personality Traits to Different Aspects of Facebook Usage, in: Hassanien, Aboul Ella/Bhatnagar, Roheet/Darwish, Ashraf (Hrsg.), Advanced Machine Learning Technologies and Applications – Proceedings of AMLTA 2020, 2020, 703-712.

Lang, Flavia/Reinbach, Hubertus, Künstliche Intelligenz im Arbeitsrecht, NZA 2023, 1273-1281.

Laumer, Sven/Maier/Christian, Oehlhorn, Caroline/Pflügner, Katharina/Weinert, Christoph/Wirth, Jakob, Digitalisierung und Zukunft der Arbeit 2020.

ders./Weitzel, Tim/Luzar, Katrin, Robo-Recruiting: Status quo und Herausforderung für die KI in der Personalgewinnung, PERSONALquaterly 2019, S. 10-15.

Lauscher, Anne/Legner, Sarah, Künstliche Intelligenz und Diskriminierung, ZfDR 2022, S. 367-390.

Lederer, Matthias/Müller-Jungnickel, Anna Maria/Pirkl, Stefanie, Künstliche Intelligenz in HR-Prozessen: Anwendungsfälle und Akzeptanzstudie für die Personaleinstellung, in: Lichtenthaler, Ulrich (Hrsg.), Künstliche Intelligenz erfolgreich umsetzen, Wiesbaden, 2021.

Leeb, Christina-Maria/Liebhaber, Johannes, Grundlagen des Datenschutzrechts, JuS 2018, S. 534-538.

Lewinski, Kai von/*Barros Fritz, Raphael* de, Arbeitgeberhaftung nach dem AGG infolge des Einsatzes von Algorithmen bei Personalentscheidungen, NZA 2018, S. 620-625.

Linardatos, Dimitrios, Auf dem Weg zu einer europäischen KI-Verordnung – ein (kritischer) Blick auf den aktuellen Kommissionsentwurf, GPR 2022, S. 58-70.

Linke, Christian, Digitale Wissensorganisation – Wissenszurechnung beim Einsatz autonomer Systeme, Baden-Baden, 2021.

ders., Wissenszurechnung beim Einsatz autonomer Systeme in Unternehmen, RDi 2021, S. 400-409.

Lischka, Konrad/Klingel, Anita, Wenn Maschinen Menschen bewerten – Internationale Fallbeispiele für Prozesse algorithmischer Entscheidung, 2017.

Lohmann, Melinda/Preßler, Theresa, Die Rechtsfigur des Erfüllungsgehilfen im digitalen Zeitalter – Ein deutsch-schweizerischer Rechtsvergleich, RDi 2021, S. 538-547.

Lopez, Paola, Bias does not equal bias: a socio-technical typology of bias in data-based algorithmic systems, Internet Policy Review 10 (2021), S. 1-29.

Lorentz, Nora, Profiling – Persönlichkeitsschutz durch Datenschutz?, Tübingen, 2020.

Lorenz, Bernd, Datenschutzrechtliche Informationspflichten, VuR 2019, S. 213-221.

Lücke, Oliver, Künstliche Intelligenz und Vorschläge zu einer EU-Regulierung, Recht und Politik 2021.

Malorny, Friederike, Auswahlentscheidungen durch künstlich intelligente Systeme, JuS 2022, S. 289-296.

dies., Datenschutz als Grenze KI-basierter Auswahlentscheidungen im Arbeitsrecht, RdA 2022, S. 170-178.

Maltzan, Stephanie von/*Käde, Lisa*, Algorithmen, die nicht vergessen – Model Inversion Attacks und deren Bedeutung für den Schutz der Daten und der Urheberrechte, DSRITB 2020, S. 505-524.

Manthey, Benjamin, Das datenschutzrechtliche Transparenzgebot, Baden-Baden, 2020.

Mantz, Reto/Marosi Johannes, in: Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, München 2019.

ders./Spittka, Jan, Anmerkung zu EuGH, Urteil v. 19.10.2016 – C-582/14 (Rs. Breyer), NJW 2016, S. 3579-3583.

Martini, Mario, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, S. 1017-1025.

ders., Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Heidelberg, 2018.

Marx, Simon/Sütthoff, Alicia, KI und Datenschutz: Zur Reichweite der Löschungspflicht des Verantwortlichen – Gewährt Art. 17 DS-GVO der betroffenen Person einen Anspruch auf Löschung der KI?, ZdiW 2022, S. 128-132.

Maschmann, Frank, Datenschutzgrundverordnung: Quo vadis Beschäftigtendatenschutz? – – Vorgaben der EU-Datenschutzgrundverordnung für das nationale Recht –, DB 2016, S. 2480-2486.

ders., Der Anspruch auf Datenkopie: ein neues Geschäftsmodell?, NZA-Beilage 2022, 50-56.

Dürig, Günter/Herzog, Roman/Scholz, Rupert (Hrsg.), Grundgesetz Kommentar, München, 2021 (zit. Dürig/Herzog/Scholz/*Bearbeiter*).

McIntosh, Shane/Nguyen, Thanh Vu (Hrsg.), 2022 ACM/IEEE 44th International Conference on Software Engineering, Piscataway, NJ 2022.

Meinecke, Dominik, Datenschutz und Data Science, Baden-Baden, 2021.

ders., Anmerkung zu EuGH, Urteil v. 30.3.2023 – C-24/21, NZA 2023, S. 487-493.

Meller-Hannich, Caroline/Hundertmark, Lukas, Rechtsschutz gegen diskriminierende „KI", in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen, 2022, S. 189-203.

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden, 2019 (zit. NK-GRC/*Bearbeiter*).

Meyermann, Alexia/Porzelt, Maike, Hinweise zur Anonymisierung von qualitativen Daten, 2014.

Mitchell, Tom M., Machine Learning, New York, 1997.

Möllers, Thomas M. J., Juristische Methodenlehre, 5. Aufl., München, 2023.

Monreal, Manfred, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO – Chancen nicht nur für das europäische Verständnis des Zweckbindungsgrundsatzes, ZD 2016, S. 507-512.

ders., Der europarechtliche Rahmen für das mitgliedstaatliche Beschäftigtendatenschutzrecht, ZD 2022, S. 359-364.

Morasch, Olga, Datenverarbeitung im Beschäftigungskontext, Baden-Baden 2018.

Mühlenbeck, Robin L., Anonyme und pseudonyme Daten, Baden-Baden 2022.

Müller, Jan-Laurin, Algorithmische Entscheidungssysteme im Nichtdiskriminierungsrecht, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen 2022, S. 205-249.

Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 23. Aufl., München 2023 (zit. ErfK/*Bearbeiter*).

Müller, Ferdinand/Kirchner, Elsa/Schüßler, Martin, Ein „KI-TÜV" für Europa? Eckpunkte einer horizontalen Regulierung algorithmischer Entscheidungssysteme, in: Kuschel, Linda/Asmussen, Sven/Golla, Sebastian J. (Hrsg.), Intelligente Systeme – intelligentes Recht – GRUR Junge Wissenschaft Hamburg 2020/2021, Baden-Baden 2021, S. 85-105.

Müller-Peltzer, Philipp/Tanczik, Valentin, Künstliche Intelligenz und Daten – Data-Governance nach der geplanten KI-Verordnung, RDi 2023, 452-458.

Nawaz, Nishad/Gomes, Anjali Mary, Artificial Intelligence Chatbots are New Recruiters, IJACSA 2019, S. 1-5.

Nebel, Maxi, Big Data und Datenschutz in der Arbeitswelt – Risiken der Digitalisierung und Abhilfemöglichkeiten, ZD 2018, S. 520-524.

Neff, Lukas, Die Zulässigkeit der Verarbeitung von Daten aus allgemein zugänglichen Quellen, DSRITB 2015, S. 81-93.

Neutatz, Felix/Abedjan, Ziawasch, What is „Good" Training Data?, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen, 2022, S. 1-15.

Ng, Annalyn/Soo, Kenneth, Data Science – was ist das eigentlich?! – Algorithmen des maschinellen Lernens verständlich erklärt, Heidelberg, 2018.

Niehoff, Maurice/Straker, Christian, Die Regulierung der Mensch-Maschine-Schnittstelle algorithmischer Entscheidungssysteme, DSRITB 2019, S. 451-465.

Niemann, Fabian/Kevekordes, Johannes, Machine Learning und Datenschutz (Teil 1), CR 2020, S. 17-25.

Niklas, Thomas/Hoffmann, Michel, Künstliche Intelligenz (KI) und Algorithmen im Arbeitsverhältnis, ArbRB 2021, S. 283-286.

ders./Thurn, Lukas, Arbeitswelt 4.0 – Big Data im Betrieb, BB 2017, S. 1589-1596.

Nink, David, Justiz und Algorithmen – Über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeiten neuer Technologien in der Rechtsprechung, 2021.

Northpointe Inc., Practitioner's Guide to COMPAS Score, 2019.

Ntoutsi, Eirini/Fafalios, Pavlos/Gadiraju, Ujwal/Iosifidis, Vasileios/Nejdl, Wolfgang/Vidal, Maria-Esther/Ruggieri, Salvatore/Turini, Franco/Papadopoulos, Symeon/Krasanakis, Emmanouil/Kompatsiaris, Ioannis/Kinder-Kurlanda, Katharina/Wagner, Claudia/Karimi, Fariba/Fernandez, Miriam/Alani, Harith/Berendt, Bettina/Kruegel, Tina/Heinze, Christian/Broelemann, Klaus/Kasneci, Gjergji/Tiropanis, Thanassis/Staab, Steffen, Bias in data-driven artificial intelligence systems – An introductory survey 2020.

Ohm, Paul, Broken promises of privacy: Responding to the surprising failure of anonymization, UCLA Law Rev. 2010, S. 1701-1777.

Orssich, Irina, Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz, EuZW 2022, S. 254-260.

Orwat, Carsten, Diskriminierungsrisiken durch Verwendung von Algorithmen, Baden-Baden 2020.

Paal, Boris/Kritzer, Ina, Geltendmachung von DS-GVO-Ansprüchen als Geschäftsmodell, NJW 2022, 2433-2439.

ders./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl., München, 2021 (zit. Paal/Pauly/*Bearbeiter*).

Panitanarak, Thap, Distributed Single-Source Shortest Path Algorithms with Two-Dimensional Graph Layout, in: Berry, Michael W./Mohamed, Azlinah/Yap, Bee Wah (Hrsg.), Supervised and Unsupervised Learning for Data Science, 2020, S. 39-58.

Petri, Thomas, Anmerkung zu EuGH, Urteil v. 8.12.2022 – C-460/22 (TU, RE ./. Google LLC), EuZW 2023, S. 139-149.

Piltz, Carlo, Die Datenschutz-Grundverordnung – Teil 3: Rechte und Pflichten des Verantwortlichen und Auftragsverarbeiters, K&R, S. 709-717.

Plath, Kai Uwe (Hrsg.), DSGVO/BDSG, 4. Aufl., 2023 (zit. Plath/*Bearbeiter*).

Plote, Maximilian Michael, Zur Entwicklung der Betriebsvereinbarung als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten, in: Arbeitsrecht im Zeitalter der Digitalisierung / Dokumentation der 9. Assistentinnen- und Assistententagung im Arbeitsrecht vom 25.-27.07.2019, Berlin 2020, S. 93-112 (zit. *Plote*, Arbeitsrecht im Zeitalter der Digitalisierung).

Ponti, Sarah/Tuchtfeld, Erik, Zur Notwendigkeit einer Verbandsklage im AGG, ZRP 2018, S. 139-141.

Pötters, Stephan, in: Thüsing, Gregor (Hrsg.), Beschäftigtendatenschutz und Compliance: effektive Compliance im Spannungsfeld von DS-GVO, BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 3. Aufl., München, 2021 (zit. *Pötters*, Beschäftigtendatenschutz).

Prietl, Bianca, Algorithmische Entscheidungssysteme revisited: Wie Maschinen gesellschaftliche Herrschaftsverhältnisse reproduzieren können, feministische studien 2019, S. 303-319.

Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen, 2015.

Räz, Tim, COMPAS: zu einer wegweisenden Debatte über algorithmische Risikobeurteilung, Forens Psychiatr Psychol Kriminol 16 (2022), S. 300-306.

Rich, Elaine, Artificial Intelligence and the Humanities, Computers and the Humanities 1985, S. 117-122.

Richardi, Reinhard (Hrsg.), Betriebsverfassungsgesetz, 17. Aufl., München, 2022 (zit. Richardi/*Bearbeiter*).

Rolfs, Christian/Giesen, Richard/Meßling, Miriam/Udsching, Peter (Hrsg.), BeckOK Arbeitsrecht, 69. Ed., München, 2023 (zit. BeckOK Arbeitsrecht/*Bearbeiter*).

Roos, Philipp/Weitz, Caspar Alexander, Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung – IT- und produktsicherheitsrechtliche Pflichten von Anbietern, Einführern, Händlern und Nutzern, MMR 2021, S. 844-850.

Rosenblat, Alex/Wikelius, Kate/boyd, danah/Gangadharan, Seeta Pena/Yu, Corrine, Data & Civil Rights: Employment Primer, SSRN Journal 2014.

Roßnagel, Alexander, Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? – Bedeutung der Grundsätze für die datenschutzrechtliche Praxis, ZD 2018, S. 339-344.

ders., Pseudonymisierung personenbezogener Daten, ZD 2018, S. 243-247.

ders., Datenlöschung und Anonymisierung – Verhältnis der beiden Datenschutzinstrumente nach DS-GVO, ZD 2021, S. 188-192.

Rostalski, Frauke, Vertrauenswürdige Verwendung von Künstlicher Intelligenz in Deutschland und Europa, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)/Rostalski, Frauke (Hrsg.), Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, Tübingen, 2022, S. 251-268.

dies./Weiss, Erik, Der KI-Verordnungsentwurf der Europäischen Kommission, ZfDR 2021, S. 329-357.

Rudin, Cynthia/Radin, Joanna, Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition, Harvard Data Science Review 1 (2019).

Rüfner, Thomas, Juristische Herausforderungen der Künstlichen Intelligenz aus der Perspektive des Privatrechts, in: Dederer, Hans-Georg/Shin, Yu-Cheol (Hrsg.), Künstliche Intelligenz und juristische Herausforderungen, Tübingen, 2021, S. 15-42.

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 9. Aufl., München 2021 (zit. MüKoBGB/*Bearbeiter*).

Santos, Guijarro, Nicht besser als nichts – Ein Kommentar zum KI-Verordnungsentwurf, ZfDR 2023, 23-41.

Schaar, Peter, Brauchen wir regulatorische Leitplanken der Digitalisierung?, in: *Klafki, Anika/Würkert, Felix/Winter, Tina* (Hrsg.), Digitalisierung und Recht – Tagung des eingetragenen Vereins Junge Wissenschaft im öffentlichen Recht an der Bucerius Law School am 26. November 2016, Hamburg, 2017, S. 29-34.

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841-1847.

ders./Wolff, Heinrich Amadeus, Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München, 2017.

Schild, Hans-Hermann, Beschäftigtendatenschutz: § 26 Abs. 1 S. 2 BDSG auf dem Prüfstand, ZD-Aktuell 2021, S. 5470.

Schlee, Nelli, EU-Kommission: Shaping Europe's Digital Future – Regulierung von KI, ZD-Aktuell 2021, 05194.

Schmidt, Bettina/Plote, Maximilian, Die Zulässigkeit der Datenverarbeitung im betrieblichen Eingliederungsmanagement, NZA 2022, S. 1297-1305.

Schmitz, Barbara/Dall'Armi, Jonas von, Datenschutz-Folgenabschätzung – verstehen und anwenden, ZD 2017, S. 57-64.

Schulz, Jimmy, Künstliche Intelligenz: Wer entscheidet über wen?, in: Kar, Resa Mohabbat/Thapa, Basanta/Parycek, Peter (Hrsg.), (Un)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2018.

Schwartmann, Rolf/Weiß, Steffen, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017 – Leitlinien für die rechtssichere Nutzung von Pseudnoymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung, 2017.

Sesing, Andreas, Grenzen systematischer Transparenz bei automatisierter Datenverarbeitung – Umfang und Grenzen der Pflicht zur Bereitstellung aussagekräftiger Informationen über die involvierte Logik, MMR 2021, S. 288-292.

ders./Baum, Kevin, Die Anforderungen an die Erklärbarkeit maschinengestützter Entscheidungen, DSRITB 2019, S. 435-451.

ders./Tschech, Angela, AGG und KI-VO-Entwurf beim Einsatz von Künstlicher Intelligenz – Einschätzung aus der Perspektive des (Anti-)Diskriminierungsrechts, MMR 2022, S. 24-30.

Simitis, Spiros, Zur Internationalisierung des Arbeitnehmerdatenschutzes – Die Verhaltensregeln der Internationalen Arbeitsorganisation, in: Hanau, Peter/Heither, Friedrich/Kühling, Jürgen (Hrsg.), Richterliches Arbeitsrecht: Festschrift für Thomas Dieterich zum 65. Geburtstag, München 1999, S. 601-627.

ders. (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., München, 2014 (zit. NK-BDSG/*Bearbeiter*).

ders./Hornung, Gerrit/Spiecker, Indra (Hrsg.), Datenschutzrecht, Baden-Baden 2019 (zit. NK-Datenschutzrecht/*Bearbeiter*).

ders./Dammann, Ulrich/Geiger, Hansjörg/Mallmann, Otto/Reh, Hans-Joachim (Hrsg.), Dokumentation zum Datenschutz mit Informationsfreiheitsrecht, Baden-Baden 2023 (zit. Spiecker gen. Döhmann/Bretthauer/*Bearbeiter*).

Söbbing, Thomas, Künstliche neuronale Netze – Rechtliche Betrachtung von Software und KI-Lernstrukturen, MMR 2021, S. 111-116.

Spiecker gen. Döhmann, Indra/Towfigh, Emanuel V., Automatisch benachteiligt – Das Allgemeine Gleichbehandlungsgesetz und der Schutz vor Diskriminierung durch algorithmische Entscheidungssysteme, Rechtsgutachten im Auftrag der Antidiskriminierungsstelle des Bundes, April 2023 (zit. *Spiecker gen. Döhmann/Towfigh*, Automatisch benachteiligt).

Spiekermann, Sarah, Zum Unterschied zwischen künstlicher und menschlicher Intelligenz und den ethischen Implikationen der Verwechslung, in: Mainzer, Klaus (Hrsg.), Philosophisches Handbuch Künstliche Intelligenz, 2020.

Spindler, Gerald, in: Hilgendorf, Eric/Roth-Isigkeit, David (Hrsg.), Die neue Verordnung der EU zur künstlichen Intelligenz, München, 2023.

ders./Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, 4. Aufl., München, 2019 (zit. Spindler/Schuster/*Bearbeiter*).

Staab, Philipp/Geschke, Sascha-Christopher, Ratings als arbeitspolitisches Konfliktfeld – Das Beispiel Zalando 2020.

Staudinger, Julius von (Hrsg.), Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Buch 2: Recht der Schuldverhältnisse, AGG (Allgemeines Gleichbehandlungsgesetz), Berlin Neubearbeitung, 2020 (zit. Staudinger (2020) Einleitung AGG/*Bearbeiter*).

ders., Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB – Buch 2: Recht der Schuldverhältnisse, Berlin 2019 (zit. Staudinger (2019)/*Bearbeiter*).

Steege, Hans, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz, MMR 2019, S. 715-721.

ders./Kuß, Christian, C. Datenschutzrecht, in: Kuß, Christian/Steege, Hans/Chibanguza, Kuuya Josef (Hrsg.), Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden, 2022.

Stefan Larsson/Fredrik Heintz, Transparency in artificial intelligence, Internet Policy Review 9 (2020).

Steinbach, Kathrin, Regulierung algorithmenbasierter Entscheidungen, Berlin, 2021.

Steven W. Knox, Machine Learning: a Concise Introduction, in: Balding, David/Cressie, Noel u.a. (Hrsg.), Wiley Series in Probability and Statistics, 2018.

Storms, Dominik, Datenschutz in der Unternehmenstransaktion, Baden-Baden, 2021.

Strassemeyer, Laurenz, Datenschutzrechtliche Transparenz von algorithmischen Entscheidungen und Verarbeitungen mittels Gamification, Ablaufdiagramme und Piktogramme, DSRITB 2019, S. 31-47.

Strecker, Michael, Bausteine einer Regulierung algorithmischer Systeme inkl. Künstlicher Intelligenz, RDi 2021, S. 124-134.

Streinz, Rudolf/Michl, Walther, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, S. 384-388.

dies. (Hrsg.), EUV/AEUV, 3. Aufl., München, 2018 (zit. EUV/AEUV/*Bearbeiter*).

Stück, Volker, Betriebsrat oder Geheimrat? – Beschäftigtendatenschutz beim Betriebsrat, ZD 2019, S. 256-261.

Stürmer, Verena, Löschen durch Anonymisieren? – Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO, ZD 2020, 626-631.

Sun, Zhensu/Li, Li/Liu, Yan/Du, Xiaoning, On the importance of building high-quality training datasets for neural code search, in: McIntosh, Shane/Nguyen, Thanh Vu (Hrsg.), 2022 ACM/IEEE 44th International Conference on Software Engineering, Piscataway, NJ 2022, S. 1609-1620.

Sydow, Gernot/Marsch, Nikolaus (Hrsg.), DS-GVO/BDSG, 3. Aufl., Baden-Baden, 2022 (zit. Sydow/Marsch/*Bearbeiter*).

Taeger, Jürgen/Gabel, Detlev (Hrsg.), DSGVO – BDSG – TTDSG, 4. Aufl., Frankfurt am Main, 2022 (zit. Taeger/Gabel/*Bearbeiter*).

ders./Pohle, Jan (Hrsg.), Computerrechtshandbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 37. Ergänzungslieferung, München, 2022 (zit. Taeger/Pohle ComputerR-HdB/*Bearbeiter*).

Teubert, Thorsten, Videointerviews zwischen Employer Branding und Digitalisierung, in: Gourmelon, Andreas (Hrsg.), Personalauswahl – ein Blick in die Zukunft, Heidelberg, 2018.

Thapa, Basanta, Vier wissenspolitische Herausforderungen einer datengetriebenen Verwaltung, in: Kar, Resa Mohabbat/Thapa, Basanta/Parycek, Peter (Hrsg.), (Un)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, S. 268-293.

Thüsing, Gregor, in: Thüsing, Gregor/Wurth, Gilbert (Hrsg.), Social Media im Betrieb, 2. Aufl., 2020.

ders./Peisker, Yannick, Datenschutzrechtliches Glasperlenspiel? – Zum Antrag des Generalanwalts Sánchez-Bordona im Verfahren Rs. C-34/21, BeckRS 2022, 24515, NZA 2023, S. 213-215.

ders./Rombey, Sebastian, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, ZD 2021, S. 548-553.

Tinnefeld, Marie-Theres/Conrad, Isabell, Die selbstbestimmte Einwilligung im europäischen Recht – Voraussetzungen und Probleme, ZD 2018, S. 391-398.

Togootogtokh, Enkhtogtokh/Amartuvshin, Amarzaya, Deep Learning Approach for Very Similar Objects Recognition Application on Chihuhua and Muffin Problem, 2018.

Traut, Johannes, Maßgeschneiderte Lösungen durch Kollektivvereinbarungen? Möglichkeiten und Risiken des Art. 88 Abs. 1 DS-GVO, RDV 2016, S. 312-319.

Trstenjak, Verica/Beysen, Erwin, Das Prinzip der Verhältnismäßigkeit in der Unionsrechtsordnung, EuR 2012, S. 265-285.

Tschider, Charlotte, Legal Opacity: Artificial Intelligence's Sticky Wicket, Iowa Law Review 2021, S. 126-162.

TÜV-Verband, Künstliche Intelligenz in Unternehmen – Chancen nutzen – Risiken begegnen, 2020.

Tversky, Amos/Kahneman, Daniel, Judgment under Uncertainty: Heuristics and Biases, Science, New Series 1974, S. 1124-1131.

Uecker, Philip, Die Einwilligung im Datenschutzrecht und ihre Alternativen, ZD 2019, S. 248-251.

ders., Extraterritorialer Anwendungsbereich der DS-GVO – Erläuterungen zu den neuen Regelungen und Ausblick auf internationale Entwicklungen, ZD 2019, S. 67-71.

Unabhängige Bundesbeauftragte für Antidiskriminierung, Vielfalt, Respekt, Antidiskriminierung – Grundlagenpapier zur Reform des Allgemeinen Gleichbehandlungsgesetzes (AGG) 2023, https://perma.cc/2CGK-YCR (archiviert am 13.08.2023).

Veale, Michael/Binns, Reuben/Edwards, Lilian, Algorithms that remember: model inversion attacks and data protection law, Philosophical Transactions 2018, S. 1-15.

ders./Borgesius, Frederik Zuiderveen, Demystifying the Draft EU Artificial Intelligence Act, Computer Law Review International 22 (2021), S. 97-112.

Veil, Winfried, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, S. 3337-3344.

Vogel, Paul, Künstliche Intelligenz und Datenschutz, Baden-Baden, 2021.

Waas, Bernd, KI und Arbeitsrecht, RdA 2022, S. 125-131.

ders., Künstliche Intelligenz und Arbeitsrecht, 2022.

Wachter, Sandra/Mittelstadt, Brent/Floridi, Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law 2017, S. 76-99.

Wagner, Gerhard, Produkthaftung für autonome Systeme, AcP 217 (2017), S. 707-765.

Waltl, Bernhard, Erklärbarkeit und Transparenz im Machine Learning, in: Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, München, 2019, S. 1-22.

Wank, Rolf, Juristische Methodenlehre – Eine Anleitung für Wissenschaft und Praxis, München, München, 2020.

Wedde, Peter, Automatisierung im Personalmanagement – arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, 2020.

Wehkamp, Nils, Weiterverarbeitung zu anderen Zwecken: Praktische Kompatibilitätsprüfung bei Zwischenspeicherung für zweckfremde Datenanalysen, DSRITB 2020, S. 215-231.

Weidenhammer, Detlef/Gundlach, Rocco, Wer kennt den „Stand der Technik"?, DuD 2018, S. 106-110.

Wennker, Phil, Künstliche Intelligenz in der Praxis – Anwendung in Unternehmen und Branchen: KI wettbewerbs- und zukunftsorientiert einsetzen, Wiesbaden 2020.

Wieder, Clemens, Datenschutzrechtliche Betroffenenrechte bei der Verarbeitung von personenbezogenen Daten mittels künstlicher Intelligenz, DSRITB 2018, S. 505-518.

Wimmer, Max, Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings, Baden-Baden, 2021.

Winter, Christian/Battis, Verena/Halvani, Oren, Herausforderungen für die Anonymisierung von Daten – Technische Defizite, konzeptuelle Lücken und rechtliche Fragen bei der Anonymisierung von Daten, ZD 2019, S. 489-493.

Wischmeyer, Thomas, Regulierung intelligenter Systeme, AöR 143 (2018), S. 1-66.

Wissenschaftsrat, Empfehlungen zur Reform des Hochschulzugangs, Drs. 5920/04 2004.

Wünschelbaum, Markus, Kollektivautonomer Datenschutz – Kollektivvereinbarungen nach Art. 88 DSGVO und ihre Gestaltungskontrolle, Tübingen, 2022.

ders., Neuer Datenschutz für betriebliche Kommunikationsdienste – Cookies, Compliance und der Abschied vom Fernmeldegeheimnis, NJW 2022, S. 1561-1566.

ders., Eckpunktepapier der Bundesregierung für ein Beschäftigtendatenschutz, MMR-Aktuell 2023, 457188.

ders., Tabula rasa im Beschäftigtendatenschutz? – EuGH setzt neue Maßstäbe: Rechtsfolgen und Handlungsoptionen – Besprechung von EuGH, Urt. v. 30.3.2023 – C-34/21, NZA 2023, S. 487-547.

Wurzberger, Sebastian, Anforderungen an Betriebsvereinbarungen nach der DS-GVO – Konsequenzen und Anpassungsbedarf für bestehende Regelungen, ZD 2017, S. 258-263.

Wybitul, Tim, Betriebsvereinbarungen im Spannungsverhältnis von arbeitgeberseitigem Informationsbedarf und Persönlichkeitsschutz des Arbeitnehmers – Handlungsempfehlungen und Checkliste zu wesentlichen Regelungen, NZA 2017, S. 1488-1494.

ders./Ströbel, Lukas, Checklisten zur DSGVO - Teil 1: Datenschutz-Folgenabschätzung in der Praxis, BB 2016, S. 2307-2311.

Zavadil, Andreas, Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen, Newsletter Datenschutzbehörde 2020.

Zech, Herbert, Künstliche Intelligenz und Haftungsfragen, ZfPW 2019, S. 198-219.

Zimmer, Mark/Stajcic, Sara, Unbewusste Denkmuster – Sollen Arbeitgeber dagegen mit Unconscious Bias Training vorgehen?, NZA 2017, S. 1040-1045.

Zweig, Katharina, Wo Maschinen irren können – Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung, 2018.

dies., Algorithmische Entscheidungen: Transparenz und Kontrolle, 2019.

dies./Krafft, Tobias, Fairness und Qualität algorithmischer Entscheidungen, in: Kar, Resa Mohabbat/Thapa, Basanta/Parycek, Peter (Hrsg.), (Un)berechenbar? – Algorithmen und Automatisierung in Staat und Gesellschaft, 2018.

digital | recht

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

Charlotte Schindler

Zulässigkeit und Grenzen algorithmischer Systeme bei arbeitsrechtlichen Auswahlentscheidungen

Die Dissertation untersucht aus einer arbeitsrechtlichen Perspektive den Einsatz algorithmischer Systeme bei Auswahlentscheidungen und berücksichtigt dabei insbesondere das Datenschutzrecht, das Allgemeine Gleichbehandlungsgesetz (AGG) und eine zukünftige Verordnung für Künstliche Intelligenz (KI-Verordnung). Ein besonderer Fokus liegt auf maschinell lernenden Systemen.