digital | recht

Staat und digitale Gesellschaft

Johannes Marosi

(Gem-)Einsame Verantwortlichkeit im Datenschutzrecht

Voraussetzungen, Folgen, Perspektiven

Band 6

Johannes Marosi

(Gem-)Einsame Verantwortlichkeit im Datenschutzrecht

Voraussetzungen, Folgen, Perspektiven

digital | recht
Staat und digitale Gesellschaft

Herausgegeben von
Prof. Dr. Matthias Bäcker, LL.M.
Prof. Dr. Roland Broemel
Prof. Dr. Thomas Burri, LL.M.
Prof. Dr. Albert Ingold
Prof. Dr. Antje von Ungern-Sternberg
Prof. Dr. Silja Vöneky

Trier, 2024

Band 6

Johannes Marosi, geboren 1986; Studium der Rechtswissenschaft an den Universitäten Münster und Oslo; Wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Dr. Matthias Bäcker an der Universität Mainz von 2016 bis 2020; Promotion 2022.
ORCID: https://orcid.org/0009-0009-6481-3485

Zugl.: Diss. iur. Fachbereich Rechts- und Wirtschaftswissenschaften, Johannes Gutenberg-Universität Mainz
vorgelegt von Johannes Marosi
Gutachter: Prof. Dr. Matthias Bäcker; Prof. Dr. Albert Ingold
Mündliche Prüfung am: 18.07.2022

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über https://dnb.d-nb.de abrufbar.

Dieses Buch steht gleichzeitig als elektronische Version über den Publikations- und Archivierungsserver Gutenberg Open Science der Universität Mainz https://openscience.ub.uni-mainz.de/ und über die Website der Schriftenreihe https://digitalrecht-oe.uni-trier.de zur Verfügung.

ISBN: 9-783759-844460
URN: urn:nbn:de:hebis:77-openscience-7bf7aaa3-ce43-427d-97f9-148a5617f5909
DOI: http://doi.org/10.25358/openscience-10591

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

Im Gedenken an Fritz

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2022 am Fachbereich 03 – Rechts- und Wirtschaftswissenschaften der Johannes-Gutenberg-Universität Mainz als Dissertation angenommen. Der Stand der Bearbeitung ist Mai 2024.

Ganz herzlich bedanke ich mich bei meinem Doktorvater und langjährigen Vorgesetzten *Professor Dr. Matthias Bäcker*, der diese Arbeit stets durch umfassende und konstruktive Anregungen und Kritik maßgeblich vorangebracht hat.

Für die rasche Erstellung des Zweitgutachtens bedanke ich mich herzlich bei *Professor Dr. Albert Ingold* und für die Übernahme des Vorsitzes bei *Professor Dr. Curt Wolfgang Hergenröder*. Ferner danke ich dem Herausgeberkreis der Schriftenreihe digital | recht für die Aufnahme als Autor. Umfängliche Danksagung gebührt auch *Prof. Dr. Louisa Specht-Riemenschneider, Dr. Reto Mantz*, *Dr. Stefan Michel*, *Simon Walkenbach* sowie alle anderen Freunden und Kollegen für ihre hilfreichen Anmerkungen zu Teilen dieser Arbeit.

Ganz herzlich danke ich natürlich auch meinen netten KollegInnen (an dem KIT) *Markus Kring*, *Tobias Fleißner*, *Hannah Lee-Wunderlich*, *Graziana Kastl-Riemann*, (an der JGU Mainz) *Eva Skobel*, *Jun.-Prof. Dr. Sebastian Golla*, *Anna Höning*, *Susanne Bauer*, *Prof. Dr. Daniela Schweigler*, *Malte Kahl*, *Erik Sollmann*, *Theresa Busch* und *Prof. Dr. Eva Ellen Wagner*, die mir stets mit fachlichem und freundschaftlichem Rat beiseite gestanden haben und dank derer ich an die Promotionszeit in Mainz und Karlsruhe als einen sehr schönen Abschnitt zurückdenken werde.

Zuletzt gilt mein großer Dank meiner gesamten Familie sowie der Familie Pick, die die Arbeit mit großer Geduld Korrektur gelesen haben und die, einschließlich meiner Partnerin Kirsten, mich immer in allen Phasen unterstützt und ermutigt haben.

Frankfurt am Main, Juli 2024 Johannes Marosi

Inhaltsübersicht

Einleitung
Einführung in das Forschungsvorhaben 1

Kapitel 1
Grundlagen zum Konzept des Verantwortlichen 15

Kapitel 2
Definitionselemente des Verantwortlichen und Abgrenzung 65

Kapitel 3
Folgen der Verantwortlichkeit 157

Kapitel 4
Gemeinsam mit anderen (Verantwortlichen) 179

Kapitel 5
Ansätze zur Überarbeitung des Konzeptes der Verantwortlichkeit 345

Kapitel 6
Zusammenfassung in Thesen 417

Inhaltsverzeichnis

Vorwort ..... *II*
Inhaltsübersicht ..... *III*
Inhaltsverzeichnis ..... *V*
Abkürzungsverzeichnis ..... *XVII*
Einleitung
Einführung in das Forschungsvorhaben 1
A. Forschungsgegenstand 1
B. Problemstellung 4
C. Aktualität 7
I. Der Verantwortliche in der Rechtsprechung 7
II. Der Verantwortliche in der Literatur 8
III. Der Verantwortliche in den Stellungnahmen der Aufsichtsbehörden 11
IV. Erkenntnisziel der Arbeit 11
D. Aufbau 12
Kapitel 1
Grundlagen zum Konzept des Verantwortlichen 15
A. Sytematik 15
I. Relevante Akteure für die Verantwortlichkeit 15
II. Der Verantwortliche und seine systematische Stellung in der DSGVO 20
1. Der Verantwortliche im Kontext seiner Pflichten und seiner Verantwortung 22
2. Der Verantwortliche im Kontext zentraler Fragen der DSGVO 26
a) Der Verantwortliche und der räumliche Anwendungsbereich 26
aa) Niederlassungsprinzip 27
bb) Marktortprinzip 29
cc) Via Völkerrecht 31
dd) Zwischenfazit 32
b) Der Verantwortliche und die Zuständigkeit der Aufsichtsbehörde 32
c) Der Verantwortliche im Bußgeldverfahren und der funktionale Unternehmensbegriff aus dem Unionskartellrecht 35
3. Fazit 35
B. Historische Entwicklung 36

I. HDSG (1970) ... 37
II. BDSG (1977) ... 41
III. OECD-Guidelines (1980) ... 44
IV. Übereinkommen Nr. 108 des Europarates (1981) ... 47
V. DSRL (1995) ... 48
VI. BDSG (2001) ... 52
1. Überblick ... 52
2. Technischer Ansatz ... 54
3. Auftragsverarbeitung ... 55
4. Dritter ... 55
5. Normadressat TMG ... 56
VII. Modernisiertes Übereinkommen Nr. 108 des Europarates (2018) ... 57
VIII. Gesetzgebung der Europäischen Union im digitalen Bereich ... 58
IX. Kritik der fehlenden Evolution des Konzeptes ... 59

Kapitel 2
Definitionselemente des Verantwortlichen und Abgrenzung ... 65
A. Bezug zur Verarbeitung ... 69
I. Verarbeitung als einheitlicher Begriff ... 70
II. Verarbeitung als einzelner Vorgang und Vorgangsreihe ... 71
B. Stelle ... 74
I. Verständnis der Aufsichtsbehörden ... 76
II. Eindeutige Bestimmung der Stelle in ihren verschiedenen Formen? ... 77
III. Person und Stelle als gegensätzliche Oberbegriffe ... 79
IV. Zurechnung des Verhaltens unterstellter Personen ... 81
V. Der Konzern als Stelle? ... 82
VI. Unternehmen mit Entscheidungsmacht außerhalb der Europäischen Union ... 89
VII. Kritik ... 91
C. Zweck(e) ... 92
D. Mittel ... 94

I. Verständnis der Aufsichtsbehörden 95
II. Wesentliche Elemente der Mittel als erforderlicher Vertragsinhalt nach Art. 28 Abs. 3 DSGVO 97
III. Die Mittel in der Rechtsprechung des EuGH 98
IV. Fazit 99
E. Entscheidung 100
I. Vorfrage: Notwendige Kenntniselemente der Entscheidung 102
1. Kenntnis der Verarbeitung personenbezogener Daten als Voraussetzung einer Verarbeitung? 103
2. Objekte der Entscheidung 104
3. Rechtsprechung des EuGH 106
4. Herleitung aus der Systematik 107
a) Kenntnis der Zwecke? 107
b) Kenntnis der Mittel? 108
c) Notwendige Kenntniselemente und Kennenmüssen bei gemeinsam Verantwortlichen 111
II. Vorfrage: Entscheidungsfähigkeit 115
III. Rechtmäßigkeit und Form der Entscheidung 116
IV. Entscheidung als technische Kontrolle der Verarbeitung? 117
V. Typologie anstatt formeller Analyse (Art. 29-Datenschutzgruppe / Europäischer Datenschutzausschuss) 120
1. Verantwortung aufgrund einer ausdrücklichen rechtlichen Zuständigkeit 121
2. Verantwortung aufgrund einer implizierten Zuständigkeit 121
3. Verantwortung aufgrund eines tatsächlichen Einflusses 123
4. Fazit der Art. 29-Datenschutzgruppe 125
5. Kritik der Typologie 126
6. Verständnis des Europäischen Datenschutzbeauftragten (EDPS) 127
F. Benennung durch (materielles) Gesetz 128

I. Entstehungsgeschichte ... 129
II. Bedeutung der Norm ... 130
III. Voraussetzungen der Benennung ... 130
IV. Qualifizierte Verantwortlichkeit als Benennung? ... 132
V. Übernahme der Normadressaten aus anderen Rechtsgebieten ... 133
VI. Vorrang der tatsächlichen Verantwortlichkeit gegenüber der rechtlichen? ... 134
VII. Anwendungsfälle? ... 136
1. TKG ... 136
2. MsbG ... 137
3. StVG ... 137
4. ATDG ... 138
5. BVerfSchG ... 140
G. Der Auftragsverarbeiter als Abgrenzungsobjekt ... 141
I. Allgemeine Voraussetzungen ... 141
II. Verständnis der Aufsichtsbehörden ... 146
III. Entscheidungsautonomie über die Mittel? ... 151
IV. Das Eigeninteresse als eigener Zweck? ... 152

Kapitel 3
Folgen der Verantwortlichkeit ... 157
A. Haftung auf Schadensersatz ... 157
I. Rechtsprechung des EuGH ... 158
II. Verständnis der Aufsichtsbehörden ... 159
B. Das Verhältnis von DSGVO und e-Commerce-RL bzw. DSA ... 160
I. Rechtslage zur DSRL ... 161
1. Haftungsprivilegierungen als Modifikation der Haftung nach Art. 82 DSGVO? ... 162
2. Haftungsprivilegierungen als Ausnahme zur Verantwortlichkeit? ... 162
3. Fazit ... 164
II. Rechtslage zur DSGVO ... 165
C. Die Verhängung von Geldbußen ... 170

I. Der funktionale Unternehmensbegriff als Maßstab 170
II. Weitere Voraussetzungen des OWiG vs. DSGVO 174
III. Fazit 177

Kapitel 4
Gemeinsam mit anderen (Verantwortlichen) 179
A. Die Quellenlage vor Geltungsbeginn der DSGVO 181
I. Literatur 181
II. Die mangelhafte Umsetzung der DSRL 182
III. Die Weiterleitung bei mehreren speicherberechtigten Stellen nach § 6 Abs. 2 BDSG a.F. als gemeinsame Verantwortlichkeit? 183
B. Rechtsprechung des EuGH 184
I. Wirtschaftsakademie 185
II. Jehovan todistajat 186
III. Fashion ID 188
IV. NZÖG (Nacionalinis visuomenes sveikatos centras) 189
V. IAB Europe 191
C. Vorfragen - „Gemeinsam" im Kontext der Definition 193
I. Art. 4 Nr. 7 vs. Art. 26 Abs. 1 S. 1 DSGVO – unterschiedliche Definitionen der gemeinsam Verantwortlichen? 194
II. Unmittelbarer Kontext: „mit anderen" 194
III. Bezugsobjekt: „entscheidet" 196
IV. Gemeinsam Verantwortliche als Rechtssubjekt sui generis? 197
D. Die Verarbeitung als Vorgangsreihe bei gemeinsam Verantwortlichen . 200
I. Divergierende Zwecke 200
II. Gemeinsame Zwecke 202
III. Möglicher Abstraktionsgrad der Zwecke 203
IV. Verhältnis zur Zweckkomplementarität 203
E. Die Zwecke der Verarbeitung als Entscheidungsobjekt 204
I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen 204
1. Das Urteil und die Schlussanträge zu Fashion ID 204
2. „Interesse" als gemeinsamer Zweck der gemeinsam Verantwortlichen? 207
3. „Interesse" als berechtigtes Interesse der gemeinsam Verantwortlichen? 209
4. „Interesse" als neues Definitionselement der gemeinsam Verantwortlichen? 210

5. „Interesse“ als Abgrenzung zum Auftragsverarbeiter? 212
6. „Interesse“ als Zweckkomplementarität 213
II. Die „Einwilligung“ in eine Verarbeitung als Einigung auf einen gemeinsamen Zweck? 216
III. Position der Aufsichtsbehörden 217
1. Europäischer Datenschutzbeauftragter (EDPS) 217
2. Europäischer Datenschutzausschuss (EDPB) 218
IV. Fazit 219
F. Die Mittel der Verarbeitung als Entscheidungsobjekt 220
I. Inhalt der Mittel? 220
II. Zugriff auf Daten oder Infrastruktur der Verarbeitung durch alle gemeinsam Verantwortlichen? 221
III. Rechtsprechung des EuGH 222
IV. Position der Aufsichtsbehörden 224
1. Art. 29-Datenschutzgruppe 224
2. Europäischer Datenschutzausschuss (EDPB) 225
3. Beispiele 226
V. Fazit 229
G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung 229
I. Verhinderung einer impliziten Billigung 233
II. Vorgang und Vorgangsreihe als Bezugsobjekt der Billigung 234
III. Zu-Eigen-Machen als Billigung oder Entscheidung? 235
IV. Die Billigung von fremden Mitteln 236
V. Stellenwert der Billigung 238
H. Die gemeinsame Entscheidung 238
I. Die reine Billigung von Zwecken und Mitteln als gemeinsame Entscheidung? 239
II. Gemeinsame Zwecke oder Mittel als Identitätsgarant der Verarbeitung 240
III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung 241
1. Prozessbezogenes Verständnis der gemeinsamen Entscheidung 243
2. Ergebnisbezogenes Verständnis der gemeinsamen Entscheidung 245
3. Das Verständnis der gemeinsamen Entscheidung nach dem Wortlaut der DSGVO 247

a) Art. 4 Nr. 7 DSGVO 247
b) Art. 26 Abs. 1 S. 1 DSGVO 248
4. Das Verständnis der gemeinsamen Entscheidung nach Auffassung der Aufsichtsbehörden 249
a) Art. 29-Datenschutzgruppe 249
b) Europäischer Datenschutzbeauftragter (EDPS) 250
c) Europäischer Datenschutzausschuss (EDPB) 251
5. Das Verständnis der gemeinsamen Entscheidung in der Rechtsprechung des EuGH 254
a) Google Spain 254
b) Jehovan todistajat 255
c) Wirtschaftsakademie 255
d) Fashion ID 258
e) NZÖG 260
6. Kritik zu dem ergebnisbezogenen Verständnis der gemeinsamen Entscheidung 261
7. Antizipierte Entscheidungsbeiträge? 263
8. Unbewusste Entscheidungsbeiträge? 264
IV. Fazit 265
I. Erheblichkeitsschwelle des Entscheidungsbeitrags 266
I. Negative Konstruktion der Erheblichkeitsschwelle 267
II. Qualitative Einschränkungen im Hinblick auf die Erheblichkeitsschwelle 269
III. Quantitative Einschränkungen im Hinblick auf die Erheblichkeitsschwelle 272
IV. Der Entscheidungsspielraum als Voraussetzung für einen Entscheidungsbeitrag 273
V. Unterlassen als Entscheidungsbeitrag? 275
VI. Rechtsprechung des EuGH 276
1. Fashion ID 278
2. Jehovan todistajat 279
3. Wirtschaftsakademie 279
4. Google Spain 282
5. Kritik 282
VII. Position der Aufsichtsbehörden 283
1. Art. 29-Datenschutzgruppe 283
2. Europäischer Datenschutzbeauftragter (EDPS) 285

3. Europäischer Datenschutzausschuss (EDPB) ... 285
VIII. Auslegungsansätze in der Literatur ... 286
IX. Fazit ... 289
J. Indizien für eine Abgrenzung zum Auftragsverarbeiter ... 289
I. Formelle Übereinkünfte und allgemeines Auftreten der Akteure ... 289
II. Art der Interaktion ... 294
III. Art der Dienstleistung ... 294
IV. Fazit ... 295
K. Auftragsverarbeiterexzess und Mitarbeiterexzess ... 296
I. Grundlagen des Auftragsverarbeiterexzesses ... 296
II. Gemeinsame Verantwortlichkeit als Folge des Auftragsverarbeiterexzesses 298
III. Funktionsübertragung und Auftragsverarbeiterexzess ... 299
IV. Gesetzliche Übermittlungspflichten des Auftragsverarbeiters ... 300
V. Mitarbeiterexzess ... 301
VI. Fazit ... 304
L. Folgen der gemeinsamen Verantwortlichkeit ... 304
I. Privilegierung der Übermittlung zwischen gemeinsam Verantwortlichen? 305
1. Wortlaut der Definition ... 306
2. Umkehrschluss aus Folgen der Verantwortlichkeit ... 307
3. Vergleich zum Auftragsverarbeiter ... 308
4. Abgrenzung der Übermittlung von einer gemeinsamen Erhebung ... 309
5. Bewertung ... 309
II. Reichweite und Anteil der individuellen Verantwortlichkeit ... 310
1. Ansatzpunkt für die Reichweite der Verantwortlichkeit ... 310
a) Der „Grad der Verantwortlichkeit“ in der Rechtsprechung des EuGH ... 312
b) Kritik des vorgangsorientierten Ansatzes ... 313
2. Anteil oder Verhältnis der Verantwortlichkeit ... 316
a) Notwendigkeit der Feststellung des Verhältnisses? ... 317
b) Kriterien für das Verhältnis der Verantwortlichkeit ... 320
3. Fazit ... 321
III. Art. 26 Abs. 3 DSGVO als „gesamtschuldnerische Verantwortlichkeit“? 322
IV. Autonome Erfüllungsfähigkeit von Pflichten? ... 326
1. Rechtsprechung des EuGH und Definition ... 326

2. Position der Aufsichtsbehörden 327
3. Erfüllungsunfähigkeit im Innenverhältnis 328
4. Konsequenzen der Erfüllungsunfähigkeit gegenüber Aufsichtsbehörden und betroffenen Personen 329
5. Fazit 329
V. Delegation von Pflichten zwischen gemeinsam Verantwortlichen 330
1. Delegationsfähigkeit von Pflichten 330
2. Konsequenz des Fehlens einer Vereinbarung 331
3. Rechtsprechung des EuGH 332
4. Position der Aufsichtsbehörden 335
5. Fazit 336
VI. Störerauswahl bei aufsichtsbehördlichen Maßnahmen 336
M. Schlussfolgerungen aus der Analyse - Die Unterkomplexität des Verantwortlichkeitskonzeptes 339
I. Neuerungen der DSGVO? 339
II. Fokus auf die betroffene Person 341
III. Breite Anwendung des Konzeptes der gemeinsamen Verantwortlichkeit durch den EuGH 342
IV. Fazit 343

Kapitel 5

Ansätze zur Überarbeitung des Konzeptes der Verantwortlichkeit 345
A. Getrennte Verantwortlichkeiten 347
B. Typologie der Verantwortlichkeit 348
C. „Datenschutzrechtliche Gesamtschuldnerschaft“ 350
D. Anwendung der DSA-Privilegierungen 351
E. Auswahlverantwortlichkeit 355
F. „Datenschutzrechtliche Beihilfe“ 357
G. Herstellerverantwortlichkeit 358
I. Frühere Ansätze 360
II. Konkrete Regelungsvorschläge 361
1. BDSG a.F. 361
2. DSGVO 362
III. Bewertung 363
H. Intermediärsverantwortlichkeit 365
I. Haushaltsausnahme 367

I. Gesetzeslage ... 368
II. Rechtsprechung des EuGH ... 369
III. Position der Aufsichtsbehörden ... 371
IV. Modernisiertes Übereinkommen Nr. 108 des Europarates ... 372
V. Kriterien für die Anwendung ... 373
VI. Konsequenzen für die Verantwortlichkeit ... 375
1. Haushaltsausnahme und (gem-)einsame Verantwortlichkeit ... 377
2. Praktikabilität einer gemeinsamen Verantwortlichkeit des Infrastrukturnutzers ... 380
3. Umfang der (gem-)einsamen Verantwortlichkeit ... 381
4. Haushaltsausnahme und Auftragsverarbeiter ... 381
VII. Fazit ... 382
J. Störerhaftung und Zweckveranlasser ... 383
I. Raum für Störerhaftung und Zweckveranlasser? ... 384
II. Rechtsprechung des EuGH ... 386
1. Folgefragen ... 387
2. Schlussanträge des Generalanwalts ... 388
III. Fazit ... 389
K. Rückgriff auf Adressaten des allgemeinen Polizei- und Ordnungsrecht 390
I. Aufsichtsbehördliche Maßnahmen als Gefahrenabwehrrecht ... 391
1. Entgegenstehende unionsrechtliche Systematik? ... 391
2. Einordnung nach deutscher Systematik ... 393
a) Ordnungsbehörde und Ordnungsrecht ... 393
b) Aufsicht sui generis? ... 396
3. Fazit ... 399
II. Adressaten im besonderen Gefahrenabwehrrecht ... 400
III. Adressaten in der DSGVO ... 402
IV. Systematische Konflikte in der DSGVO ... 405
V. Materiell-rechtliche Pflichtigkeit des Verantwortlichen ... 407
VI. Adressaten in der DSRL ... 409
VII. Fazit ... 412
L. Ausblick ... 413

Kapitel 6
Zusammenfassung in Thesen ... 417
A. Zu Kapitel 1: Grundlagen zum Konzept des Verantwortlichen ... 417

B. Zu Kapitel 2: Definitionselemente des Verantwortlichen und Abgrenzung 418
C. Zu Kapitel 3: Folgen der Verantwortlichkeit 420
D. Zu Kapitel 4: Gemeinsam mit anderen (Verantwortlichen) 421
E. Zu Kapitel 5: Ansätze zur Überarbeitung des Konzeptes der Verantwortlichkeit 424

Literaturverzeichnis *427*

Abkürzungsverzeichnis

a.	auch
a.A.	andere(r) Ansicht
Abs.	Absatz
a.E.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AfP	Zeitschrift für Medien- und Kommunikationsrecht
API	Application Programming Interface (englisch)
Art.	Artikel
ATDG	Antiterrordateigesetz
Aufl.	Auflage
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BayLfD	Bayerischer Landesbeauftragter für den Datenschutz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
BeckRS	beck-online.RECHTSPRECHUNG
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern, für Bau und Heimat
BNetzA	Bundesnetzagentur
BR-Drs.	Bundesratsdrucksache
bspw.	beispielsweise
BT-Drs.	Bundestagsdrucksache
BTLJ	Berkeley Technology Law Journal
BverfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BYOD	Bring your own device

BVwVfG	Bundesverwaltungsverfahrensgesetz
bzgl.	bezüglich
bzw.	beziehungsweise
CLSR	Computer Law & Security Review
COM	Europäische Kommission
CR	Computer und Recht
DA	Data Act (englisch)
DAR	Deutsches Autorecht
DDG	Digitale-Dienste-Gesetz
DGA	Data Governance Act (englisch)
DMA	Digital Markets Act (englisch)
DÖV	Die öffentliche Verwaltung
DSA	Digital Services Act (englisch)
DSB	Datenschutz-Berater
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DSRL	Datenschutzrichtlinie
DSRL-JI	Datenschutzrichtlinie für Justiz und Inneres
DuD	Datenschutz und Datensicherheit
E	Entwurf
ebd.	ebenda
e-Commerce-RL	Richtlinie über den elektronischen Geschäftsverkehr
EDPB	Europäischer Datenschutzausschuss (im Deutschen auch EDSA)
EDPS	Europäischer Datenschutzbeauftragter (im Deutschen auch EDSB)
EEA	Europäischer Wirtschaftsraum (englisch)
EG	Europäische Gemeinschaft
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
ePrivacy-RL	Datenschutzrichtlinie für elektronische Kommunikation
ERA Forum	Journal of the Academy of European Law
ErwGr	Erwägungsgrund
etc.	et cetera

ETIAS	Europäisches Reiseinformations- und -genehmigungssystem (englisch)
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuGRZ	Europäische Grundrechte-Zeitschrift
EuR	Europarecht (Zeitschrift)
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
f., ff.	folgende, fortfolgende
Fn.	Fußnote(n)
GbR	Gesellschaft bürgerlichen Rechts
GDPR	Datenschutzgrundverordnung (englisch)
gem.	gemäß
gen.	genannt
GewArch	Gewerbearchiv
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
ggü.	Gegenüber
GmbH	Gesellschaft mit beschränkter Haftung
GRCh	Charta der Grundrechte der Europäischen Union
grds.	Grundsätzlich
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
GVBl.	Gesetz- und Verordnungsblatt
HDSG	Hessisches Datenschutzgesetz
HmbBfDI	Hamburger Beauftragter für den Datenschutz und die Informationsfreiheit
Hrsg.	Herausgeber
Hs.	Halbsatz
HSOG	Hessisches Sicherheits- und Ordnungsgesetz
IDPL	International Data Privacy Law
i.E.	im Ergebnis
IHK	Industrie- und Handelskammer

IoT	Internet of Things
Inc.	Incorporated (anglo-amerikanische Gesellschaftsform)
InfoSoc-RL	Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft
insb.	insbesondere
Int'l J. Comm. L. & Pol'y	International Journal of Communications Law & Policy
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
IT	Informationstechnologie
ITRB	IT-Rechtsberater
i.V.m.	in Verbindung mit
JIPITEC	Journal of Intellectual Property, Information Technology and Electronic Commerce Law
JZ	JuristenZeitung
K&R	Kommunikation & Recht
KMU	Kleine und mittlere Unternehmen
LbauO	Landesbauordnung
LfV	Landesamt für Verfassungsschutz
LG	Landgericht
lit.	littera
LKA	Landeskriminalamt
Ltd.	Limited (anglo-amerikanische Gesellschaftsform)
MBO	Musterbauordnung
MJ	Maastricht Journal of European and Comparative Law
MMR	Zeitschrift für IT-Recht und Recht der Digitalisierung
MsbG	Messstellenbetriebsgesetz
m.w.N.	mit weiteren Nachweisen
m.W.v.	mit Wirkung von
NJW	Neue Juristische Wochenschrift
No	Nummer (englisch)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht

OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLG	Oberlandesgericht
OSI	Open Systems Interconnection
OSP	Online Service Provider
OVG	Oberverwaltungsgesetz
OwiG	Ordnungswidrigkeitengesetz
PinG	Privacy in Germany
POG	Polizei- und Ordnungsbehördengesetz
ProdSG	Produktsicherheitsgesetz
RdV	Recht der Datenverarbeitung
RL	Richtlinie
RLP	Rheinland-Pfalz
Rn.	Randnummer
RW	Rechtwissenschaft (Zeitschrift)
S.	Satz (bei Normen), sonst Seite (bei Quellenangaben)
SaaS	Software as a Service
SDK	Software Development Kit (englisch)
StVG	Straßenverkehrsgesetz
SächsPBG	Sächsisches Polizeibehördengesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TB	Tätigkeitsbericht
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
u.a.	unter anderem
u.ä.	und ähnliche(s)
ULD	Unabhängiges Landeszentrum für Datenschutz
US	Vereinigte Staaten (englisch)
USA	Vereinigte Staaten von Amerika (englisch)
usw.	und so weiter
v.	von/vom

v.a.	vor allem
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VO	Verordnung
Vorbem.	Vorbemerkung
VRRL	Verbraucherrechterichtlinie
vs.	versus
VuR	Verbraucher und Recht
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WP	Working Paper
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz

Im Übrigen wird auf *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 10. Aufl., Berlin 2021, verwiesen.

Einleitung

Einführung in das Forschungsvorhaben

A. Forschungsgegenstand

> „*For an effective system of data protection it is of great importance that the role, rights, and responsibilities of the various persons and parties involved be stated unambigously.*“[1]

Diese Arbeit befasst sich mit dem Verantwortlichen[2] gem. Art. 4 Nr. 7 Datenschutzgrundverordnung[3] („DSGVO“). Sie versteht den Verantwortlichen als primären Normadressaten im Datenschutzrecht. Er ist der primär Verpflichtete, aber auch Berechtigte des Datenschutzrechts.[4] Somit ist der Verantwortliche einer der konzeptionellen Dreh- und Angelpunkte der DSGVO.[5]

Elementarer Bezugspunkt für den Verantwortlichen ist seine Verarbeitung von Daten.[6] Grundsätzlich soll jede Verarbeitung einen Verantwortlichen haben.[7] Eine Anwendbarkeit des Datenschutzrechts ohne einen Verantwortlichen scheint kaum denkbar.[8] Denn ohne Verantwortlichen existiert für zahlreiche Pflichten der DSGVO schlicht kein Adressat. Der Verantwortliche definiert sich anhand seiner organisatorischen Entscheidungshoheit über einen Verarbeitungsvorgang, spezifisch über dessen Zwecke und Mittel. Eine technische Beherrschbarkeit dieses Vorgangs ist nicht unbedingt erforderlich.[9] Folglich setzt die Verantwortlichkeit auch nicht eine Art von „Besitz“ oder eine unmittelbare Zugriffsmöglichkeit auf die verarbeiteten

[1] *Hondius*, Emerging data protection in Europe, 1975, 101.

[2] In dieser Arbeit werden geschlechtsspezifische Formen aus Gründen der Lesbarkeit und des gesetzestreuen Wortlauts verwendet. Diese Formen beziehen sich aber stets auf Personen jeden Geschlechts.

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates 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).

[4] Vgl. *Lewinski/Herrmann*, ZD 2016, 467, 469.

[5] Für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 18.

[6] Dazu: Kapitel 2 A. Bezug zur Verarbeitung.

[7] Simitis/*Dammann*, § 3 BDSG a.F., Rn. 224.

[8] Daher widmet sich diese Arbeit auch nicht dem rein theoretischen Problem einer Verarbeitung ohne Verantwortlichem.

[9] Dazu: Kapitel 2 E. Entscheidung.

personenbezogenen Daten voraus. Mit der Entscheidungshoheit über einen Verarbeitungsvorgang geht die Kontrolle über diesen einher. Aus dieser Kontrolle erwächst die Verantwortlichkeit des Verantwortlichen. An diese Verantwortlichkeit wiederum knüpfen die Pflichten des Verantwortlichen sowie dessen Haftung an.[10]

Sofern nur ein Akteur im Zusammenhang mit einem Verarbeitungsvorgang auftritt oder mit diesem befasst ist, ist die Bestimmung des Verantwortlichen regelmäßig unproblematisch. Denn wenn nur ein Akteur diesen Verarbeitungsvorgang veranlasst oder beherrscht, dann trifft er notwendigerweise die Entscheidung über die Zwecke und Mittel dieses Verarbeitungsvorgangs. Es gibt dann keine anderen Akteure, die mitentscheiden könnten oder an die Teilaspekte der Verarbeitung delegiert sein könnten. Soweit das Datenschutzrecht grundsätzlich einen Verantwortlichen als Normadressaten voraussetzt, erübrigt sich in diesem Szenario regelmäßig die Prüfung der tatbestandlichen Voraussetzungen der Verantwortlichkeit. Im deutschen Datenschutzrecht herrschte darüber hinaus lange die Ansicht, dass selbst in Verarbeitungsszenarien mit mehreren Akteuren grundsätzlich ein Akteur allein Verantwortlicher sei.[11] Falls mehrere Akteure im Zusammenhang mit einem Verarbeitungsvorgang auftraten oder mit diesem befasst waren, wurde je nach Szenario eine Auftragsverarbeitung oder eine Übermittlung zwischen Verantwortlichen angenommen. Daher wurden die spezifischen, tatbestandlichen Voraussetzungen des Verantwortlichen gem. Art. 4 Nr. 7 DSGVO[12] zunächst mangels praktischer Anwendungsfälle, später trotz zunehmend starker Vernetzung der Akteure aufgrund der vorherrschenden Meinung in Rechtsprechung und Literatur kaum relevant.

Tatsächlich ist neben der Abgrenzung des Verantwortlichen zum Auftragsverarbeiter auch die Abgrenzung von alleinigen, singulären oder separaten[13] Verantwortlichen zu gemeinsam Verantwortlichen im Rahmen stetig zunehmender Vernetzung und Spezialisierung einzelner Akteure immer wichtiger geworden. Um aber eine gemeinsame Verantwortlichkeit überhaupt zu erkennen, ist es zunächst notwendig, die tatbestandlichen Voraussetzungen hierfür zu verstehen. Denn soweit zumindest ein Verantwortlicher bereits zweifelsfrei vorhanden ist, könnte der andere Akteur auch ein Auftragsverarbeiter, ein separater Verantwortlicher oder aber datenschutzrechtlich irrelevant sein. Diese Einordnung ist deswegen so wichtig, weil sie

[10] *Lewinski/Herrmann*, ZD 2016, 467, 469.

[11] Deutlich wird das v.a. in den deutschen Vorinstanzen der Rechtssache Wirtschaftsakademie (dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[12] Bzw. seiner Vorgängernormen.

[13] Die Bezeichnung als separater Verantwortlicher erfolgt dabei in Szenarien mit mehreren Akteuren in Abgrenzung zu gemeinsam Verantwortlichen.

die Rechtsstellung der beteiligten Akteure prägt. Denn zwischen den Rollen gemeinsam Verantwortlicher, Auftragsverarbeiter und separater Verantwortlicher bestehen unterschiedliche Pflichten sowie Haftungsrisiken. So gelten bei einer gemeinsamen Verantwortlichkeit die besonderen Anforderungen des Art. 26 DSGVO.

Die gemeinsame Verantwortlichkeit bestimmt sich über die allgemeinen tatbestandlichen Voraussetzungen des Verantwortlichen unter Hinzufügung des Definitionselementes „gemeinsam". Gemeinsam Verantwortliche müssen gemäß der Definition „gemeinsam [über Zwecke und Mittel der Verarbeitung] entscheiden". Maßgebliche Voraussetzung der gemeinsamen Verantwortlichkeit ist also die „gemeinsame Entscheidung". Trotz bislang fünf verschiedener Urteile des EuGH[14] scheinen die genauen Voraussetzungen der gemeinsamen Verantwortlichkeit, und damit indirekt auch der Verantwortlichkeit selbst, bislang nicht abschließend geklärt zu sein. Ziel dieser Arbeit ist daher zunächst eine Untersuchung der Voraussetzungen der Verantwortlichkeit, insbesondere der gemeinsamen Verantwortlichkeit. Dabei wird versucht eine Systematik hinter den Urteilen des EuGH zur gemeinsamen Verantwortlichkeit zu erkennen. Gleichermaßen werden aber auch die Defizite dieser vermeintlichen Systematik betont.

Ziel der Arbeit ist es die Voraussetzungen der einzelnen Definitionselemente des Verantwortlichen darzustellen. Dies erfolgt sowohl für die Form des singulär Verantwortlichen wie auch für die gemeinsam Verantwortlichen. Dabei werden auch die Wechselwirkungen zwischen den Voraussetzungen und Folgen der Verantwortlichkeit untersucht. Zum Schluss der Arbeit werden verschiedene Ansätze für eine Überarbeitung des Konzeptes der datenschutzrechtlichen Verantwortlichkeit dargestellt und bewertet.

Ausführungen zum Auftragsverarbeiter sowie den Aufsichtsbehörden erfolgen ausschnittweise dort, wo es in Abgrenzung zum bzw. im Zusammenhang mit dem Verantwortlichen notwendig wird. Ebenso wird die betroffene Person ausschnittweise in ihrer Rolle als Berechtigte gegenüber dem Verantwortlichen betrachtet.

Diese Arbeit verwendet, außerhalb eines konkreten historischen Kontextes, zur besseren Verständlichkeit grundsätzlich den Begriff des „Verantwortlichen"[15] so wie ihn die DSGVO in Art. 4 Nr. 7 vorsieht. Daneben bezieht sich der Begriff „für die Verarbeitung Verantwortlicher" auf Art. 2 lit. d der Richtlinie 95/46/EG[16] bzw.

[14] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[15] Vgl. zur Begriffskürzung: Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 2.

[16] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Datenschutzrichtline („DSRL“) und der Begriff „verantwortliche Stelle“ auf § 3 Abs. 7 des Bundesdatenschutzgesetzes a.F.[17] („BDSG a.F.“) Der Begriff „gemeinsame Verantwortlichkeit“ bezeichnet im Folgenden eine unbestimmte Anzahl von gemeinsam Verantwortlichen, jedoch nicht ein eigenes Rechtssubjekt neben den individuellen gemeinsam Verantwortlichen.[18]

B. Problemstellung

> *„Jede Datenschutzregelung hat [...] von Anfang an unter dem Vorbehalt einer sich ständig weiterentwickelnden Informations- und Kommunikationstechnologie gestanden.“*[19]

Das Konzept der Verantwortlichkeit im Datenschutzrecht stammt, wie die meisten Konzepte des Datenschutzrechts, aus der Zeit der ersten Datenschutzgesetze der frühen 1970er Jahre.[20] Es wurde zu einer Zeit entwickelt, in der Datenverarbeitungen in Ermangelung eines „Personal Computers“ (PC) vor allem in Großrechneranlagen durch den Staat oder große Unternehmen durchgeführt wurden.[21] Der Verantwortliche schien als Normadressat im ersten deutschen Datenschutzgesetz, dem Hessischen Datenschutzgesetz („HDSG“) 1970, so offensichtlich, dass er nicht einmal gesondert definiert wurde.[22] Erst im BDSG 1977 wurde die „speichernde Stelle“ legaldefiniert.[23] Die größte Änderung erfuhr das Konzept der Verantwortlichkeit dann durch das Definitionselement der „Entscheidung über die Verarbeitung“ im Rahmen der DSRL.[24]

Um größtmögliche Rechtssicherheit für die Anwender zu gewährleisten, sollte ein Konzept wie die Verantwortlichkeit grundsätzlich nicht vom technischen Fortschritt

---

[17] Bundesdatenschutzgesetz a.F. in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66) zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618) m.W.v. 09.11.2017.

[18] Dazu: Kapitel 4 C. Vorfragen - „Gemeinsam“ im Kontext der Definition.

[19] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 87.

[20] *Roßnagel*, MMR 2005, 71, 71; *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, 199 ff.

[21] *Albers*, § 62 Datenschutzrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, [4]2020, Rn. 2.

[22] Dazu: Kapitel 1 B. I. HDSG (1970).

[23] Dazu: Kapitel 1 B. II. BDSG (1977).

[24] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 87 attestiert dem BDSG 1990 vorher noch ein weitgehendes Übergehen der technischen Veränderungen seit dem ersten BDSG 1977.

abhängig sein. Es sollte also technikneutral sein. Allerdings bewirkte gerade der technische Fortschritt in der Datenverarbeitung einen immensen Wandel von isolierten Datenverarbeitungen durch einzelne, klar abgrenzbare Akteure hin zu stark vernetzten, interdependenten und dezentralen Verarbeitungen.[25] Daher stellt sich berechtigterweise die Frage, ob das Konzept der Verantwortlichkeit wirklich so technikneutral ist, dass es dem heutigen Stand der Verarbeitungsrealität noch gerecht wird.[26] Ebenso sollte hinterfragt werden, ob es sich beim Konzept der Verantwortlichkeit überhaupt um ein technikneutrales Konzept handelt oder ob sich dieses nicht vielmehr an den technischen Rahmenbedingungen seiner Entstehungszeit orientierte.[27] Es lässt sich in jedem Fall feststellen, dass eine Verarbeitung mittlerweile nicht mehr notwendigerweise nur einem einzelnen Akteur zugewiesen werden kann oder muss.[28] Eine der drängendsten Fragen bei datenschutzrechtlichen Sachverhalten ist heutzutage regelmäßig: welche Rollen nehmen die verschiedenen an einer Verarbeitung beteiligten Akteure überhaupt wahr?[29]

Abseits der Frage, wie technikneutral das Konzept der Verantwortlichkeit ist, muss ebenso hinterfragt werden, wie entwicklungsfähig es ist.[30] Ausgehend vom Definitionselement der Entscheidung und damit einhergehend der Kontrolle handelt es sich bei der Verantwortlichkeit um ein grundsätzlich hierarchisches Konzept. Eine Kooperation von verschiedenen Akteuren sah das Datenschutzrecht lange, wenn überhaupt, nur im Rahmen einer Übermittlung zwischen verschiedenen Verantwortlichen voraus. Auch hinsichtlich des Konzeptes des Auftragsverarbeiters geht das Datenschutzrecht aufgrund von dessen Weisungsgebundenheit von einem hierarchischen Konzept aus. Das Konzept von mehreren, gemeinsam Verantwortlichen für eine Verarbeitung wurde erst sehr spät im Gesetzgebungsprozess der DSRL

[25] So betont Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 87 m.w.N. insbesondere die Auswirkungen der Dezentralisierung für die Zuordnung der Verantwortung. Vgl. a. *Roßnagel*, MMR 2005, 71, 71.

[26] Simitis/*Dammann*, § 3 BDSG a.F., Rn. 2, 224.

[27] Vgl. *Alsenoy*, CLSR[28] (2012), 25, 27 f.; vgl. *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 9. Fragend, ob es sich beim BDSG 1990 um eine flexible und offene Regelung des Datenschutzes handelt: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 87.

[28] Vgl. *Lewinski/Herrmann*, ZD 2016, 467, 468.

[29] *Alsenoy*, CLSR[28] (2012), 25, 25.

[30] Vgl. hierzu: *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 71 ff. Vgl. *Lewinski/Herrmann*, ZD 2016, 467, 468 f. zum Dreieck „Verantwortliche Stelle - Betroffener – Datenschutzaufsicht". Vgl. zur Perspektive der systematischen Digitalisierung: *Spiecker gen. Döhmann*, CR 2016, 698, 700 f.

überhaupt aufgenommen.[31] Dieses Konzept der gemeinsamen Verantwortlichkeit schien bis zu dem Urteil des EuGH[32] in Wirtschaftsakademie Schleswig-Holstein (im Folgenden „Wirtschaftsakademie")[33] in Praxis und Literatur quasi nicht existent zu sein. Insbesondere im deutschen Datenschutzrecht wurden bis zu den Entscheidungen des EuGH – wie die Vorlagefragen in den Rechtssachen Wirtschaftsakademie und Fashion ID zeigen – vor allem die Fragen einer Auswahlverantwortlichkeit[34] oder zivilrechtlichen Störerhaftung[35] diskutiert. Die gemeinsame Verantwortlichkeit fristete ein eher theoretisches Dasein und fand sich nicht einmal explizit in der damaligen deutschen Umsetzung von Art. 2 lit. d DSRL, dem § 3 Abs. 7 BDSG a.F.

Aufgrund der spezifischen Voraussetzung der Weisungsgebundenheit für den Auftragsverarbeiter einerseits,[36] der bislang unklaren und scheinbar flexiblen Voraussetzungen für gemeinsam Verantwortliche andererseits, droht der gemeinsamen Verantwortlichkeit nun eine Auffangfunktion zuzukommen. Diese Auffangfunktion stünde aber im Widerspruch zu den gegenüber der Auftragsverarbeitung härteren Folgen einer Verantwortlichkeit.[37] Daher muss der Unionsgesetzgeber langfristig eine Lösung finden, die sowohl die Grundrechte bzw. Interessen der Verantwortlichen wie auch der betroffenen Personen berücksichtigt.[38]

Das Konzept der Verantwortlichkeit sieht sich folglich mit zwei elementaren Fragen konfrontiert. Das ist zum einen die Frage, ob es die Verarbeitungsrealität noch adäquat abbilden kann und zum anderen, ob das momentane Verständnis der gemeinsamen Verantwortlichkeit mehr als nur eine Übergangslösung[39] darstellen kann. Dazu ist es notwendig, die genauen Voraussetzungen der Verantwortlichkeit generell, ebenso wie auch die Grenzen der gemeinsamen Verantwortlichkeit auszuloten.

---

[31] Dazu: Kapitel 1 B. V. DSRL (1995).

[32] Zu den Entscheidungen: Kapitel 4 B. Rechtsprechung des EuGH.

[33] EuGH-Entscheidungen werden hier zur besseren Lesbarkeit mit ihrer üblichen Verschlagwortung zitiert, regelmäßig also dem Klagegegner im Vorlagebeschluss.

[34] Dazu: Kapitel 5 E. Auswahlverantwortlichkeit.

[35] Dazu: Kapitel 5 J. Störerhaftung und Zweckveranlasser.

[36] Dazu: Kapitel 2 G. Der Auftragsverarbeiter als Abgrenzungsobjekt.

[37] Vgl. zur Auftragsverarbeitung: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 2.

[38] Vgl. für das deutsche Recht: „Treffen [...] zwei grundrechtlich geschützte Rechtspositionen aufeinander, so ist es in erster Linie Aufgabe des einfachen Gesetzgebers, eine ausgleichende sachgerechte Lösung des Konflikts zu finden." BVerwG, Urteil vom 16.03.1989 – 4 C 36.85 = BVerwGE[81] 1990, 329, 343.

[39] Dabei könnte man an die Rechtsprechung des EuGH in EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857 zur Niederlassung gem. Art. 4 Abs. 1 lit. a DSRL und die Einführung des Marktortprinzips durch Art. 3 Abs. 2 DSGVO denken. So wurde scheinbar das weite Verständnis des EuGH im Hinblick auf die Niederlassung gem. DSRL durch die Einführung des Marktortprinzips in der DSGVO überflüssig gemacht.

C. Aktualität

Beim Konzept des Verantwortlichen handelt es sich aufgrund seiner zentralen Bedeutung[40] für das Datenschutzrecht als dessen primär Verpflichteter[41] grundsätzlich um ein konstant aktuelles Thema. Denn durch das Zusammenspiel des Konzeptes der Verarbeitung mit dem Konzept des Verantwortlichen bestimmen sich die wesentlichen Pflichten der DSGVO.[42] Durch neue Verarbeitungsszenarien stellen sich dabei immer wieder Fragen zu den Verantwortlichkeitsrollen der beteiligten Akteure. Dieses zeigen die folgenden Ausführungen zum Verantwortlichen in der Rechtsprechung, Literatur und in den Stellungnahmen der Aufsichtsbehörden.

I. Der Verantwortliche in der Rechtsprechung

In jüngerer Zeit hat der EuGH unter anderem entschieden, dass die für das Amtsblatt eines Mitgliedstaates zuständige Einrichtung, die Rechtsakte und amtliche Dokumente unverändert veröffentlicht, trotz fehlender Rechtspersönlichkeit als Verantwortlicher anzusehen ist, sofern Zwecke und Mittel der durch das Amtsblatt vorgenommenen Verarbeitungen durch das nationale Recht vorgegeben sind.[43] Daneben ergingen Urteile zur gemeinsamen Verantwortlichkeit bei fehlender Beauftragung einer App[44] sowie im Kontext eines Regelungsrahmens für die Versteigerung von Online-Werbeplätzen[45]. Denkbar sind weitere Entscheidungen zur Verantwortlichkeit auch im Anwendungsbereich der Datenschutzrichtlinie für Justiz und Inneres[46] („DSRL-JI") im Hinblick auf gemeinsame Dateien der Sicherheitsbehörden.[47] So lag dem EuGH zwischenzeitlich eine Vorlage des VG Wiesbaden zur Frage der Verantwortlichkeit bei dem INPOL-System der Polizei vor.[48]

Daneben bestehen auch innerhalb der Systematik der DSGVO Unklarheiten im

[40] Dazu: Kapitel 1 A. II. Der Verantwortliche und seine systematische Stellung in der DSGVO.
[41] Vgl. Art. 5 Abs. 2 DSGVO.
[42] Für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 1, 18.
[43] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265.
[44] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209.
[45] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328.
[46] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 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.
[47] Dazu: Kapitel 2 F. VII. Anwendungsfälle?; vgl. Simitis/*Dammann*, § 3 BDSG a.F., Rn. 2.
[48] VG Wiesbaden, Beschluss vom 30.07.2021 – 6 K 421/21 = CR 2021, 732. Zur Rücknahme: *Schild*, ZD-Aktuell 2022, 01264.

Zusammenhang mit dem Konzept der Verantwortlichkeit. Dies galt beispielweise bis vor kurzem für die Verhängung von Geldbußen nach Art. 83 DSGVO gegenüber dem Verantwortlichen und das Verhältnis des Konzeptes der Verantwortlichkeit zum nationalen Strafrecht. Hier hat der EuGH auf eine Vorlage des KG Berlin hin entschieden.[49] Unter welchen Bedingungen zudem eine datenschutzrechtliche Störerhaftung abseits der Verantwortlichkeit bestehen kann, ist bislang bestenfalls ansatzweise geklärt.[50]

Ein weites Verständnis des Verantwortlichen war spätestens seit der Entscheidung des EuGH in Google Spain, in dem der EuGH geurteilt hatte, dass Suchmaschinenbetreiber selbstständige Verantwortliche darstellen,[51] absehbar.[52] Einzelne Kommentatoren rügten bereits bei diesem Urteil die Unterkomplexität der datenschutzrechtlichen Verantwortlichkeit und deren fehlende Weiterentwicklung im Rahmen der DSGVO.[53] Dennoch schienen die Urteile des EuGH zur gemeinsamen Verantwortlichkeit in den Rechtssachen Wirtschaftsakademie, Jehovan todistajat und Fashion ID[54] trotz der Tatsache, dass die Ansätze dieser Rechtsprechung bereits in der Rechtssache Google Spain erkennbar waren, viele überrascht zu haben.[55] Um ein Verständnis dieser Rechtsprechung wird in der datenschutzrechtlichen Literatur immer noch gerungen.[56] Aber auch die Auswirkungen von dem Urteil in der Rechtssache Google Spain im Hinblick auf Intermediäre und ihre Einordnung als Verantwortliche scheinen noch nicht abschließend geklärt.[57]

II. Der Verantwortliche in der Literatur

Neben den aktuellen Entwicklungen in der Rechtsprechung zur Verantwortlichkeit ist auch die Kritik am Konzept der Verantwortlichkeit selbst nicht neu. So stellte *Abel* bereits für das BDSG 2001 fest, dass ein Kulturwandel von einem negatorischen

[49] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203.

[50] Kapitel 5 J. Störerhaftung und Zweckveranlasser.

[51] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 41.

[52] Vgl. *Kollmar*, NVwZ 2019, 1740, 1740.

[53] *Masing*, https://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/ (abgerufen am 17.07.2024) These 7.

[54] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[55] Auch die deutschen Gerichte dürfte das weite Verständnis des EuGH zur gemeinsamen Verantwortlichkeit überrascht haben, wenn man die Vorlagefragen in Wirtschaftsakademie und Fashion ID betrachtet. Denn die Vorlagefragen gingen entweder von gar keiner Verantwortlichkeit aus oder hielten diese jedenfalls nicht für zwingend.

[56] Dazu: Kapitel 4.

[57] *Keller*, BTLJ[33] (2018), 287, 323, 336.

Schrankendenken[58] auf ein Denken in Datenverkehrsregeln und Verantwortlichkeiten notwendig sei.[59] Trotzdem ende der Blick auf die Geschichte des Datenschutzes (bis 2003) in Deutschland auf einer „ewigen Baustelle".[60] *Wedde* ging sogar so weit zu fragen, ob die damalige und auch noch heutige Form der Verantwortungszuweisung vor dem Hintergrund der damaligen technischen Entwicklung im Informations- und Kommunikationsbereich noch eine Zukunft habe.[61] Eine eindeutige Zuweisung der Verantwortlichkeit lasse sich abseits autonomer und nicht digitalisierter Anwendungen kaum noch treffen.

Walz attestierte dem traditionellen Regelungsmodell der Verantwortlichkeit (seit dem ersten BDSG 1977, also der speichernden bzw. später verantwortlichen Stelle) bereits im Jahr 2000 zahlreiche Defizite.[62] Unberücksichtigt blieben etwa der Konzernsachverhalt oder die Fernwartung. Gemeinsame Dateien mehrerer speichernder Stellen würden im BDSG 1990 nur am Rande erwähnt und die Begriffe „Netz" oder „Vernetzung" kenne das Gesetz schließlich gar nicht. Den wirtschaftlichen und informationstechnologischen Veränderungen müsse mit einem grundlegend neuen Datenschutzmodell begegnet werden.[63]

Ebenso bemängelte *Roßnagel* 2005 eine Zersplitterung der Verantwortlichkeit durch eine Vielzahl beteiligter Akteure, die spontane Ver- und Entnetzung und ständige Rollenwechsel.[64] Es entstehe eine zunehmende Verantwortungsdiffusion[65]. Pflichten nur den Verantwortlichen aufzuerlegen sei nicht mehr ausreichend, auch die Technikgestalter müssten verpflichtet werden.[66]

Auch *Dammann* hielt für die verantwortliche Stelle in § 3 Abs. 7 BDSG a.F. noch 2014, also vor der Verabschiedung der DSGVO, fest, dass sich die Reformdiskussion auf die Frage konzentriere, ob das Konzept noch der heutigen IT-Wirklichkeit gerecht werde.[67] Ein erheblicher und stetig wachsender Anteil der Verarbeitungen sei durch ein

[58] Damit bezog er sich wohl vor allem auf den sogenannten Verbotsgrundsatz.

[59] *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 54.

[60] *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 59.

[61] *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 78.

[62] *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 457.

[63] *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 457 f.

[64] *Roßnagel*, MMR 2005, 71, 72.

[65] Vgl. zum Begriff: *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 40 f.

[66] Dazu: Kapitel 5 G. Herstellerverantwortlichkeit; *Roßnagel*, MMR 2005, 71, 74 f.

[67] Simitis/*Dammann*, § 3 BDSG a.F., Rn. 2.

komplexes Zusammenwirken mehrerer Akteure mit ganz unterschiedlichen Kompetenzen und Interessen gekennzeichnet. Dabei sei auch die Autorenschaft für die jeweiligen Daten nicht mehr immer eindeutig bestimmbar.

Nicht unerwähnt sollte zudem bleiben, dass allein nach Abgabe dieser Arbeit vier verschiedene Dissertationsschriften zum Themenkomplex der Verantwortlichkeit, insbesondere der gemeinsamen Verantwortlichkeit, erschienen sind. Diese sind soweit möglich noch berücksichtigt worden. Während sich die Dissertation von *Kosmider*[68] zwar allgemein und bündig mit den Voraussetzungen der Verantwortlichkeit beschäftigt und hierbei etwa die Rechtfertigung der Verarbeitungen innerhalb der Sphäre des Verantwortlichen erörtert, liegt der primäre Fokus der Arbeit aber auf der Verhängung von Geldbußen durch Aufsichtsbehörden und dem zugrundeliegenden Zurechnungsmodell von Verstößen. Auch die Dissertation von *Schneider*[69] beschäftigt sich zwar mit den Voraussetzungen der Verantwortlichkeit, hat ihren primären Fokus aber auf dem Innenverhältnis von gemeinsam Verantwortlichen, also der nach Art. 26 Abs. 1 DSGVO zu schließenden Vereinbarung sowie Ansprüchen aus dem Innenverhältnis. Die Dissertation von *Radtke*[70] versucht die gemeinsame Verantwortlichkeit umfänglich in deren Voraussetzungen sowie Folgen in der Form der Vereinbarung, dem Außenverhältnis gegenüber betroffenen Personen, den aufsichtsbehördlichen Maßnahmen und dem Innenverhältnis zu beleuchten, kann aber aufgrund dieses Zuschnittes nicht durchgehend eine tiefergehende Analyse bieten. Die zuletzt erschiene Dissertationen von *Wittner*[71] widmet sich der gemeinsamen Verantwortlichkeit unter Berücksichtigung der Plattformökonomie sowie des grundrechtlichen Rahmens, insbesondere des Schutzgutes von Art. 8 GrCH. Nach einer bündigen Analyse der Verantwortlichkeit wird dann als Lösungsansatz eine noch näher zu definierende Plattformverantwortlichkeit sowie eine gestufte Verantwortlichkeit im Sinne einer primären und sekundären Verantwortlichkeit entwickelt. Soweit ersichtlich wird in all den genannten Werken allerdings keine detaillierte Analyse der Definitionselemente der Verantwortlichkeit durchgeführt, so dass der Ansatz dieser Arbeit nach wie vor gewinnbringend erscheint.

[68] *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021.
[69] *Schneider*, Gemeinsame Verantwortlichkeit, 2021.
[70] *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021.
[71] *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022.

III. Der Verantwortliche in den Stellungnahmen der Aufsichtsbehörden

Auch die Art. 29-Datenschutzgruppe[72] hielt 2010 in ihrem Working Paper[73] 169 („WP 169“) zum Verantwortlichen und Auftragsverarbeiter fest, dass die konkrete Anwendung der Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ immer schwieriger werde. So werde das Umfeld von Verarbeitungen immer komplexer und die Entwicklung der Informations- und Telekommunikationstechnologie führe zusammen mit der Globalisierung zu einer immer stärkeren organisatorischen Differenzierung.[74] Der Kontext einer Datenverarbeitung sei zum Zeitpunkt der Unterzeichnung des Übereinkommens Nr. 108 des Europarates 1981 und weitgehend auch zum Zeitpunkt der Verabschiedung der DSRL 1995 noch recht klar und überschaubar gewesen. Dies habe sich jedoch geändert. Insbesondere durch die Entwicklung und Einführung von Produkten und Diensten der neuen Informations- und Kommunikationstechnologien entstünden neue Rollen und Verantwortlichkeiten, deren Wechselbeziehung mit bestehenden oder sich entwickelnden Verantwortlichkeiten nicht immer klar sei.[75] Wenn es aber nicht ausreichend klar sei, wer welcher Verpflichtung unterliege – weil etwa niemand verantwortlich sei oder es mehrere mögliche Verantwortliche gebe – dann bestehe das offensichtliche Risiko, dass nur unzureichende oder überhaupt keine Maßnahmen durch die Aufsichtsbehörden ergriffen würden. Folglich bliebe das Datenschutzrecht wirkungslos. Unklarheiten in der Auslegung [der Verantwortlichkeit] könnten zu konkurrierenden Forderungen und anderen Kontroversen führen. Daher müsse ausreichende Klarheit geschaffen werden, um eine wirksame Anwendung und Einhaltung des Datenschutzes in der Praxis zu ermöglichen und sicherzustellen.

IV. Erkenntnisziel der Arbeit

Die vorliegende Arbeit soll zum Verständnis der Verantwortlichkeit einen Beitrag leisten, indem sie die einzelnen Definitionselemente des Verantwortlichen untersucht, ein systematisches Verständnis der Rechtsprechung des EuGH zur Verantwortlichkeit

---

[72] Gem. Art. 29 DSRL ein Beratungsgremium bestehend aus Vertretern der Aufsichtsbehörden der EU-Mitgliedstaaten, des Europäischen Datenschutzbeauftragten und der Europäischen Kommission.

[73] Bei den Working Papers der Art. 29-Datenschutzgruppe handelt es sich um Auslegungshilfen zu einzelnen Themen der DSRL und teilweise auch der DSGVO.

[74] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 3, 8.

[75] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 8.

anbietet und Lösungsansätze für die vorher identifizierten Defizite des Konzeptes der Verantwortlichkeit diskutiert. Dies stellt einen ersten kritischen Schritt zur Überarbeitung und Weiterentwicklung des Konzeptes der datenschutzrechtlichen Verantwortlichkeit dar.

D. Aufbau

Diese Arbeit besteht aus einer Einleitung sowie sechs Kapiteln. Die vorliegende Einleitung endet mit diesem Unterkapitel zum Aufbau (D.) der Arbeit. Das zweite Kapitel der Arbeit widmet sich den Grundlagen zum Konzept des Verantwortlichen. Hier wird die Systematik (A.) der Verantwortlichkeit innerhalb der DSGVO dargestellt sowie die historische Entwicklung (B.) des Konzeptes der Verantwortlichkeit. Das zweite Kapitel der Arbeit beschäftigt sich mit den Definitionselementen des Verantwortlichen und der Abgrenzung zum Auftragsverarbeiter. Dabei orientiert sich der Aufbau dieses Kapitels an der Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO (B.-E.). Ebenso wird der Bezug zur Verarbeitung (A.), die Benennung eines Verantwortlichen durch (materielles) Gesetz (F.) sowie die Abgrenzung zum Auftragsverarbeiter (G.) analysiert. Das dritte Kapitel der Arbeit beschäftigt sich mit bestimmten Folgen der Verantwortlichkeit. Dazu zählen die Haftung auf Schadensersatz (A.), das Verhältnis von DSGVO und e-Commerce-RL bzw. DSA (B.) sowie die Verhängung von Geldbußen (C.). Das vierte Kapitel der Arbeit beschäftigt sich mit dem Konzept der gemeinsamen Verantwortlichkeit. Zunächst wird die Quellenlage zu diesem Thema vor dem Geltungsbeginn der DSGVO (A.) betrachtet. Danach erfolgt ein Überblick über die Rechtsprechung des EuGH zu der gemeinsamen Verantwortlichkeit (B.). Im Anschluss werden Vorfragen zu dem Definitionselement „gemeinsam“ im Kontext der Definition (C.) sowie die Vorgangsreihe bei gemeinsam Verantwortlichen (D.) erörtert. Darauf folgend werden die Zwecke der Verarbeitung als Entscheidungsobjekt erörtert (E.). In diesem Kontext erfolgt eine Analyse des Begriffs „Interesse“ in der Rechtssache Fashion ID sowie eine Darstellung des Konzeptes der Zweckkomplementarität. Ebenso werden die Mittel der Verarbeitung als Entscheidungsobjekt erörtert (F.). Im Zusammenhang mit dem Konzept der Zweckkomplementarität wird sodann die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung (G.) diskutiert. Danach wird die gemeinsame Entscheidung (H.) sowie die Erheblichkeitsschwelle eines dafür notwendigen Entscheidungsbeitrags (I.) untersucht. Anschließend werden Indizien für eine Abgrenzung zum

Auftragsverarbeiter (J.) sowie der Auftragsverarbeiter und Mitarbeiterexzess im Hinblick auf die gemeinsame Verantwortlichkeit (K.) analysiert. Dieser Teil der Arbeit endet mit einer Betrachtung der Folgen der gemeinsamen Verantwortlichkeit (L.) sowie Schlussfolgerungen aus der Analyse der gemeinsamen Verantwortlichkeit (M.). Das fünfte Kapitel der Arbeit beschäftigt sich mit verschiedenen Ansätzen zur Überarbeitung des Konzeptes der Verantwortlichkeit, unter anderem der Herstellerverantwortlichkeit (G.), der Haushaltsausnahme (I.), der Störerhaftung und dem Zweckveranlasser (J.) sowie einem Rückgriff auf die Adressaten des allgemeinen Polizei- und Ordnungsrechts (K.). Er endet mit einem Ausblick auf die weitere Entwicklung (L.). Im sechsten Kapitel der Arbeit werden schließlich die wesentlichen Thesen zusammengefasst dargestellt.

Kapitel 1

Grundlagen zum Konzept des Verantwortlichen

Der folgende Teil stellt die systematischen und historischen Grundlagen für diese Arbeit dar. Im Rahmen der systematischen Grundlagen werden die relevanten Akteure der DSGVO beschrieben und eine Analyse der systematischen Stellung des Verantwortlichen vorgenommen. Dabei soll die Darstellung der systematischen Grundlagen zu einem Verständnis der Wechselwirkungen zwischen den verschiedenen Akteuren beitragen. Ebenso soll das Konzept der Verantwortlichkeit in ein Verhältnis zu den anderen datenschutzrechtlichen Konzepten, wie etwa dem räumlichen Anwendungsbereich, gesetzt werden. Im Rahmen der historischen Grundlagen erfolgt eine chronologische Darstellung der maßgeblichen deutschen, europäischen sowie internationalen datenschutzrechtlichen Gesetze, Richtlinien, Verträge oder Empfehlungen. Abgeschlossen wird dies mit einer Analyse der bisherigen Entwicklung, um die historische Anpassungsfähigkeit des Konzeptes zu bewerten.

A. Sytematik

I. Relevante Akteure für die Verantwortlichkeit

Die DSGVO definiert eine Vielzahl von Akteuren mit unterschiedlichen Funktionen. Die für das Konzept der Verantwortlichkeit relevanten Akteure werden hier überblicksartig dargestellt.[1]

Zunächst gibt es den singulären[2] oder einzelnen „Verantwortlichen“ gem. Art. 4 Nr. 7 DSGVO:

> *„die natürliche oder juristische Person [...] oder andere Stelle, die allein [...] über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.*

[1] Vgl. a. Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 7.

[2] Im Sinne von einzelnen, also nicht gemeinsam Verantwortlichen. *Marx/Sütthoff*, CR 2023, 29, 30 ff. sprechen daneben noch von der getrennten Verantwortlichkeit. Hierbei handelt es sich allerdings nur um separate Verantwortliche in einem Verarbeitungskontext mit mehreren Akteuren.

In Art. 24 DSGVO („Verantwortung des für die Verarbeitung Verantwortlichen") werden weitere Details zum Verantwortlichen geregelt. Allerdings legt die Norm keine Voraussetzungen, sondern nur Pflichten des Verantwortlichen fest. So normiert Art. 24 DSGVO, dass der Verantwortliche technische und organisatorische[3] Maßnahmen zu treffen hat, um die Einhaltung der DSGVO zu gewährleisten und dass er entsprechende Nachweise hierfür erbringen muss. Zusammen mit Art. 25, 32 und 35 DSGVO wird damit der Pflichtenkreis des Verantwortlichen konkreter bestimmt.[4] In der DSRL-JI wird der Verantwortliche nahezu identisch in Art. 3 Nr. 8 definiert, wobei hier allerdings nur die zuständige Behörde als Subjekt angesprochen wird. Die Entsprechung für Art. 24 DSGVO findet sich in Art. 19 DSRL-JI.

Darüber hinaus gibt es den „gemeinsam Verantwortlichen" gem. Art. 4 Nr. 7 DSGVO:

> *„die natürliche oder juristische Person [...] oder andere Stelle, die [...] gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet".*

Der maßgebliche Unterschied zum singulären Verantwortlichen liegt hierbei darin, dass nicht nur eine, sondern mindestens zwei Personen bzw. (organisatorische) Stellen an der Entscheidung beteiligt sind. Näheres zu den gemeinsam Verantwortlichen regelt Art. 26 DSGVO. Allerdings werden auch dort die Voraussetzungen nicht konkreter normiert. Stattdessen wird die Definition aus Art. 4 Nr. 7 DSGVO in leicht veränderter Form[5] wiederholt. Daneben werden bestimmte Pflichten und Rechtsfolgen an das Vorliegen einer gemeinsamen Verantwortlichkeit geknüpft.[6] Auch der gemeinsam Verantwortliche wird in Art. 3 Nr. 8 DSRL-JI definiert, ergänzt durch das Pendant zu Art. 26 DSGVO in Art. 21 DSRL-JI.[7]

Ein weiterer wichtiger Akteur ist der „Auftragsverarbeiter"[8] gem. Art. 4 Nr. 8

[3] Diese organisatorischen Maßnahmen können auch in der internen Zuweisung von Verantwortlichkeiten bestehen, vgl. für das BDSG a.F.: Simitis/*Ernestus*, § 9 BDSG a.F., Rn. 22. Insofern kann man auch den Vertrag nach Art. 28 Abs. 3 DSGVO oder die Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO als organisatorische Maßnahme begreifen.

[4] Kühling/Buchner/*Hartung*, Art. 24 DS-GVO, Rn. 1.

[5] Kapitel 4 C. I. Art. 4 Nr. 7 vs. Art. 26 Abs. 1 S. 1 DSGVO – unterschiedliche Definitionen der gemeinsam Verantwortlichen?

[6] Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 9, 11.

[7] Zur gemeinsamen Verantwortlichkeit in der DSRL-JI: *Radtke*, JIPITEC[11] (2020), 242.

[8] Dieser wurde in der deutschen Literatur zum BDSG a.F. auch häufig als Auftragsdatenverarbeiter bezeichnet.

DSGVO:

> *„eine natürliche oder juristische Person [...] oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".*

Ausgehend vom Wortlaut scheint der maßgebliche Unterschied zum Verantwortlichen darin zu liegen, dass der Auftragsverarbeiter im Auftrag des Verantwortlichen handelt. Wenn man allerdings Art. 29 DSGVO hinzuzieht, wird klar, dass der Auftragsverarbeiter nicht nur im Auftrag, sondern grundsätzlich auch nur auf Weisung des Verantwortlichen hin personenbezogene Daten verarbeitet. Details der Auftragsverarbeitung regelt Art. 28 DSGVO. Wichtig für das Verhältnis zum Verantwortlichen ist hier insbesondere Art. 28 Abs. 10 DSGVO. Dieser regelt, dass ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher gilt.[9] Nach Art. 28 Abs. 2, 4 DSGVO sind auch ein Unterauftragsverarbeiter sowie theoretisch ein Unterunterauftragsverarbeiter[10] usw. denkbar. Dazu bedarf es allerdings der Genehmigung des Verantwortlichen. In der DSRL-JI wird der Auftragsverarbeiter in Art. 3 Nr. 8 identisch zur DSGVO definiert. Den Art. 28 und 29 DSGVO entsprechen Art. 22 und 23 DSRL-JI.

Daneben gibt es noch den „Dritten" gem. Art. 4 Nr. 10 DSGVO:

> *[Der Dritte ist] „eine natürliche oder juristische Person [...] oder andere Stelle,* ***außer*** *der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;"*[11]

Der Begriff des Dritten dient als Negativabgrenzung zum Begriff des Verantwortlichen und des daran anknüpfenden Auftragsverarbeiters.[12] Soweit nicht

---

[9] Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[10] Vgl. Kühling/Buchner/*Hartung*, Art. 28 DS-GVO, Rn. 85.

[11] Hervorhebung durch den Autor.

[12] Kühling/Buchner/*Hartung*, Art. 4 Nr. 10 DS-GVO, Rn. 1, 5, 8; Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 277; Paal/Pauly/*Ernst*, Art. 4 DSGVO, Rn. 59 f.; BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 109; eingeschränkt: G/S/S/V/*Veil*, Art. 4 Nr. 10 DSGVO, Rn. 1, 12 ff. Für die DSRL: vgl. BT-Drs., 12/8329, S. 14; Ehmann/Helfrich DSRL, Art. 2, Rn. 54; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 23 f. Kuner/Bygrave/Docksey/*Tosoni*, Art. 4 (10) GDPR, 171, ergänzt durch Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 44 weist darauf hin, dass der

einer der in der Definition genannten Akteure im Hinblick auf eine konkrete Verarbeitung vorliegt, handelt es sich um einen Dritten. Darüber hinaus werden durch diese Definition dem Verantwortlichen und Auftragsverarbeiter auch die unter ihrer unmittelbaren Verantwortung verarbeitenden Personen zugeschrieben. Folglich legt die Definition des Dritten indirekt die Verantwortlichkeits- bzw. Kontrollsphäre des Verantwortlichen[13] fest. Damit hilft vor allem die Definition des Dritten, wenn auch lediglich indirekt, bei der Bestimmung anderer Verantwortlichkeitssphären und somit anderer Verantwortlicher.[14] Von dieser Verantwortlichkeitssphäre erfasst und damit privilegiert im Hinblick auf den Datenumgang sind die betroffene Person[15], der Verantwortliche, der Auftragsverarbeiter sowie diesen i.S.v. Art. 29 DSGVO unterstellte[16] Personen oder Stellen.[17] Diese benötigen keine eigene Verarbeitungsrechtfertigung[18] nach Art. 6 Abs. 1 DSGVO und haben, sofern nicht anderweitig festgelegt,[19] keine, denen des Verantwortlichen entsprechenden, Pflichten.

Begriff auch zur Abgrenzung zum Begriff des Empfängers dient. Ähnlich wohl: BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 102.

[13] Der Auftragsverarbeiter wiederum verarbeitet nur im Auftrag des Verantwortlichen.

[14] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 7 f., 37 f.; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 89 mit Beispielen. So enthielt der geänderte Vorschlag der Kommission zur Vorgängerregelung der DSRL Erläuterungen dazu, dass aufgrund der Definition des Dritten kein Konzernprivileg gegeben ist: Ehmann/Helfrich DSRL, Art. 2, Rn. 55 ff., vgl. a. Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 5; *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 20, 22; zu den praktischen Folgen (unter BDSG a.F.): *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 52.

[15] Zu Überlegungen, ob die betroffene Person sich selbst gegenüber Verantwortlicher sein kann: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 226; *Marx/Sütthoff*, CR 2023, 29, 33 f.

[16] Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 125 und Sydow/Marsch/*Ingold*, Art. 4 Nr. 8 DSGVO, Rn. 151; Sydow/Marsch/*Ingold*, Art. 29 DSGVO, Rn. 4 f.; Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 281, 288 ff.; Paal/Pauly/*Martini*, Art. 29 DSGVO, Rn. 14 f.; mit weiteren Beispielen: Taeger/Gabel/*Lutz/Gabel*, Art. 29 DSGVO, Rn. 9; Ehmann/Selmayr/*Bertermann*, Art. 29 DS-GVO, Rn. 3 ff. Kühling/Buchner/*Hartung*, Art. 4 Nr. 10 DS-GVO, Rn. 9 und Kühling/Buchner/*Hartung*, Art. 29 DS-GVO, Rn. 13 sehen im Grunde nur Freelancer, freiberufliche Mitarbeiter und Berater als Anwendungsfall.

[17] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 30; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 78, 88. Nach ebd., Rn. 19 Fn. 11 sind dies etwa die Angestellten einer Organisation, nach ebd., Rn. 88 aber auch vergleichbare „Rollen" (dazu: Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 43).

[18] Art. 6 Abs. 1 DSGVO spricht von Bedingungen. Häufig wird auch der Begriff Rechtsgrundlage verwendet. Hinsichtlich der Selbstkontrolle des Verantwortlichen liegt aber der Begriff Verarbeitungsrechtfertigung näher.

[19] Etwa wie individuell per Norm beim Auftragsverarbeiter.

Neben dieser Bestimmung anderweitiger Verantwortlichkeit[20] dient der Begriff des Dritten vor allem auch als Tatbestandsmerkmal für die Pflichten des Verantwortlichen.[21] Der Dritte wird in der DSRL-JI nicht definiert.

Zu erwähnen ist auch der „Empfänger" gem. Art. 4 Nr. 9 DSGVO:

> *„eine natürliche oder juristische Person [...] oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht."*

Diese Definition stellt einen übergeordneten Begriff gegenüber den anderen Bezugssubjekten in der DSGVO dar.[22] Sie dient nicht zur Abgrenzung zu anderen Rollen, sondern als rein faktische Beschreibung.[23] Die DSGVO behandelt den Empfänger demnach weniger als Adressat für bestimmte Pflichten als vielmehr als ein Tatbestandsmerkmal,[24] das die Pflichten des Verantwortlichen und Auftragsverarbeiters beschreibt.[25] In der DSRL-JI wird der Empfänger in Art. 3 Nr. 10 definiert.

Daneben enthält Art. 4 DSGVO noch weitere Definitionen von Subjekten und Objekten, die allerdings nicht eine Verantwortlichkeit positiv oder negativ beschreiben, sondern Tatbestandsmerkmale bestimmter Normen darstellen. Dazu gehören die Definition der Hauptniederlassung, des Vertreters, des Unternehmens, der Unternehmensgruppe und der internationalen Organisation.

---

[20] Vgl. Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 10 DSGVO, Rn. 4; Ehmann/Selmayr/*Klabunde/Horvath*, Art. 4 DS-GVO, Rn. 49. Für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 18: „Die Eigenschaft einer Person als Empfänger oder Dritter bemißt [sic] sich im Verhältnis zu ihm [dem für die Verarbeitung Verantwortlichen]"; siehe a. Beispiel 26 in *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 38.

[21] In der DSGVO findet man den Dritten etwa bei den berechtigen Interessen in Art. 6 Abs. 1 lit. f DSGVO sowie daran anknüpfend den Informationspflichten in Art. 13 Abs. 1 lit. d DSGVO und 14 Abs. 2 lit. b DSGVO. Vgl. für die DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 37; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 24.

[22] Kühling/Buchner/*Hartung*, Art. 4 Nr. 9 DS-GVO, Rn. 1, 4 f.

[23] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 92.

[24] Etwa in Art. 14, 15, 30 DSGVO.

[25] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 85 auch mit Bezug auf den Dritten; G/S/S/V/*Veil*, Art. 4 Nr. 9 DSGVO, Rn. 1 ff., 14; Auernhammer/*Eßer*, Art. 4 DSGVO, Rn. 91; Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 9 DSGVO, Rn. 1. Für die DSRL: Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 18; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 25.

Die maßgeblichen Definitionen der DSRL, also des „für die Verarbeitung Verantwortlichen“ gem. Art. 2 lit. d DSRL, des „Auftragsverarbeiters“ gem. Art. 2 lit. e DSRL, des „Dritten“ gem. Art. 2 lit. f DSRL und des „Empfängers“ gem. Art. 2 lit. g DSRL sind alle im Wesentlichen, bis auf geringfügige sprachliche Unterschiede, identisch mit denen der DSGVO. Daher lässt sich, mangels inhaltlicher Änderungen an den Definitionen des Verantwortlichen sowie des gemeinsam Verantwortlichen,[26] die Rechtsprechung wie auch Literatur zu Art. 2 lit. d DSRL grundsätzlich auf die DSGVO übertragen.[27] Dies gilt insbesondere auch für die Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ der Art. 29-Datenschutzgruppe,[28] besser bekannt als WP 169. Dies gilt jedenfalls soweit, wie sich durch Art. 26 DSGVO und die neueren „Guidelines 07/2020 on the concepts of controller and processor in the GDPR“[29] (im Folgenden „Leitlinien zum Verantwortlichen“) des EDPB[30] keine Änderungen ergeben.

II. Der Verantwortliche und seine systematische Stellung in der DSGVO

Der Begriff des Verantwortlichen taucht in der DSGVO 474 Mal, in der DSRL 56 Mal auf.[31] Dabei wird er jeweils in Art. 4 Nr. 7 DSGVO und Art. 2 lit. d DSRL definiert. Im Gegensatz zum sachlichen und räumlichen Anwendungsbereich in Art. 2 und 3 DSGVO bzw. Art. 3 und 4 DSRL gibt es keine vergleichbare Norm für den persönlichen Anwendungsbereich der DSGVO oder der DSRL.[32] Somit gibt es also grundsätzlich keine Norm in DSGVO oder DSRL, die den Verantwortlichen allgemein als Adressat der Verordnung bzw. Richtlinie festlegt. Er ist zunächst einmal nur legaldefiniert. In diesem Unterkapitel soll daher analysiert werden, inwiefern dem

[26] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 11.

[27] EuGH, Urteil vom 17.06.2021 – C-597/19 (Mircom/Telenet) = GRUR 2021, 1067, Rn. 107; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 47 Fn. 18; *Alsenoy*, JIPITEC 7 (2016), 271, Rn. 2 Fn. 11; *Golland*, K&R 2019, 533, 534; *Schreiber*, ZD 2019, 55, 55; deutlich: *Monreal*, CR 2019, 797, Rn. 4.

[28] Also dem Vorgängergremium des EDPB gem. Art. 68 DSGVO.

[29] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021.

[30] Der Europäische Datenschutzausschuss (EDSA bzw. englisch EDPB) besteht aus den Leitern bzw. deren Vertretern der Aufsichtsbehörden der Mitgliedstaaten sowie des Europäischen Datenschutzbeauftragten. Er ist in Art. 68 ff. DSGVO geregelt. Gem. Art. 70 Abs. 1 lit. e DSGVO erlässt er Leitlinien zwecks Sicherstellung einer einheitlichen Anwendung der DSGVO.

[31] Jeweils einschließlich der Erwägungsgründe.

[32] Vgl. für das BDSG a.F.: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 14.

Verantwortlichen auf systematischer Ebene eine zentrale Rolle in der DSGVO,[33] auch abseits einer expliziten Benennung als allgemeinem Adressaten der DSGVO, zukommt. Dabei werden zum einen die Pflichten und die Verantwortung, die dem Verantwortlichen ausdrücklich per Norm auferlegt werden, betrachtet. Zum anderen wird untersucht, ob das Konzept des Verantwortlichen eine maßgebliche Rolle bei zentralen Fragen, wie etwa dem räumlichen Anwendungsbereich, der DSGVO spielt. Soweit dem Verantwortlichen eine solche zentrale Rolle in der Systematik der DSGVO zukommt, könnte er auch dort als Normadressat angenommen werden, wo ein Normadressat nicht explizit genannt wird.

An den Verantwortlichen knüpfen vier grundlegende Pflichten an.[34] So ist der Verantwortliche verpflichtet:

- die „Grundsätze für die Verarbeitung personenbezogener Daten“ gem. Art. 5 Abs. 2 DSGVO zu erfüllen,[35]
- die Betroffenenrechte nach Art. 12 ff. DSGVO zu erfüllen,
- mit den Aufsichtsbehörden gem. Art. 31 DSGVO zusammenzuarbeiten,
- im Falle einer rechtswidrigen Verarbeitung gegebenenfalls gegenüber der betroffenen Person Schadensersatz zu leisten gem. Art. 82 DSGVO.

Darüber hinaus verpflichten eine Vielzahl von Normen den Verantwortlichen direkt oder indirekt durch Verweis auf andere Normen. Ebenso lässt sich anhand des Verantwortlichen auch der Kreis der Personen feststellen, die unter seiner Verantwortung zum Umgang mit den Daten befugt sind.[36] Auf einer abstrakteren Ebene weist *van Alsenoy* der Qualifizierung einer Stelle[37] als Verantwortlicher (oder Auftragsverarbeiter) die folgenden Implikationen zu:[38]

- die Zuordnung von Verantwortlichkeit und Haftung,

[33] So etwa: Auernhammer/*Eßer*, Art. 4 DSGVO, Rn. 77. Für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 18.

[34] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 9; *Hanloser*, ZD 2019, 455, 458; ähnlich: S/J/T/K/*Schwartmann/Mühlenbeck*, Art. 4 DSGVO, Rn. 129; vgl. für die DSRL: ErwGr 25 DSRL; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 3, 5 f.

[35] Ehmann/Selmayr/*Klabunde/Horvath*, Art. 4 DS-GVO, Rn. 41.

[36] *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 22.

[37] Im Original: „Entity“.

[38] *Alsenoy*, CLSR[28] (2012), 25, 26.

- die Feststellung des anwendbaren Rechts,[39]
- die Einhaltung der wesentlichen Normen.

Dabei sollen der Verantwortliche (und Auftragsverarbeiter) die Basis für die Zuordnung von Verantwortlichkeit darstellen.[40]

In den Worten der Art. 29-Datenschutzgruppe dient der Begriff „für die Verarbeitung Verantwortlicher" in erster Linie dazu, zu bestimmen, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und wie die betroffenen Personen ihre Rechte in der Praxis ausüben können.[41] Anders ausgedrückt: Er diene dazu, Verantwortung zuzuweisen.[42] Normen, die dem Verantwortlichen Verantwortung zuweisen, gelten grundsätzlich für singuläre wie auch gemeinsam Verantwortliche. Die Erfüllung aller Verpflichtungen muss daher auch bei gemeinsam Verantwortlichen sichergestellt sein.[43]

1. Der Verantwortliche im Kontext seiner Pflichten und seiner Verantwortung

Soweit der Begriff des Verantwortlichen dazu dient, Verantwortung zuzuweisen, muss diese Zuweisung durch Normen auch erfolgen. Ohne diese Zuweisung handelt es sich bei dem Begriff des Verantwortlichen nur um einen legaldefinierten Begriff, der erst noch mit Bedeutung aufgeladen werden muss.[44] Auch hinsichtlich der etymologischen Bedeutung des Begriffs des Verantwortlichen stellt sich die Frage, wofür er verantwortlich ist. Selbst durch den Begriff des für die Verarbeitung Verantwortlichen nach DSRL ergeben sich nicht notwendigerweise konkrete Pflichten. Innerhalb der Systematik der DSGVO ist der Verantwortliche zwar sicherlich der primäre Normadressat, mangels expliziter Festlegung aber nicht der allgemeine Adressat der gesamten Verordnung.

Eine der zentralen Normen der DSGVO ist Art. 5 DSGVO. In dieser Norm werden

---

[39] Der Aufsatz wurde vor EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857 veröffentlicht. Ähnlich a. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 6 f.; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 18; *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 20.

[40] *Alsenoy*, CLSR[28] (2012), 25, 27.

[41] Vgl. ErwGr 25 DSRL.

[42] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 6.

[43] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 29; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 9.

[44] *Mantz*, ZD 2014, 62, 64 f.

in Abs. 1 die Grundsätze für die Verarbeitung personenbezogener Daten festgehalten. In Abs. 2 wird dem Verantwortlichen die Verantwortung für die Einhaltung des Abs. 1 zugewiesen. Diese Einhaltung muss er im Rahmen der sogenannten Rechenschaftspflicht (Accountability) nachweisen können.

Einer der Grundsätze der Verarbeitung ist gem. Art. 5 Abs. 1 lit. a DSGVO die Rechtmäßigkeit der Verarbeitung. Diese Rechtmäßigkeit der Verarbeitung könnte man zunächst als globale Verpflichtung des Verantwortlichen verstehen.[45] Der Verantwortliche könnte dann also nicht gegen die DSGVO verstoßen, ohne gleichzeitig den Grundsatz der Rechtmäßigkeit der Verarbeitung zu verletzen. Verstünde man den Grundsatz der Rechtmäßigkeit global, wäre aber auch jeder Verstoß des Verantwortlichen gegen die DSGVO einheitlich über Art. 83 Abs. 5 lit. a DSGVO sanktioniert. Die Ausdifferenzierung der unterschiedlichen Verstöße gegen die DSGVO in Art. 83 Abs. 4 bis 6 DSGVO wäre überflüssig. Aufgrund der erheblichen Bußgeldandrohung in Art. 83 Abs. 5 lit. a DSGVO liegt es daher näher die Rechtmäßigkeit der Verarbeitung im Sinne von Art. 6 Abs. 1 DSGVO zu verstehen.[46] Eine Verarbeitung bedarf zu ihrer Rechtmäßigkeit also einer Verarbeitungsrechtfertigung gem. Art. 6 Abs. 1 DSGVO.[47] Der Grundsatz der Rechtmäßigkeit zeigt sich auch in den verschärften Voraussetzungen für eine Verarbeitungsrechtfertigung für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO. Hinsichtlich der anderen Grundsätze der Verarbeitung könnte man zwar auch auf eine globale Verpflichtung des Verantwortlichen schließen, allerdings finden diese Grundsätze vielfach ihre konkrete Ausgestaltung in spezifischen Normen der DSGVO.[48] Dies gilt etwa für den Grundsatz der Transparenz der Verarbeitung nach Art. 5 Abs. 1 lit. a DSGVO im Rahmen der Betroffenenrechte nach Art. 12-15 DSGVO. In diesen Normen wird der Verantwortliche wiederum explizit als Normadressat genannt. Folglich kann man zusammenfassend aus Art. 5 Abs. 2 DSGVO nicht den persönlichen Anwendungsbereich der DSGVO ableiten.

Daneben könnte noch Art. 24 DSGVO, aufgrund des Normtitels „Verantwortung des für die Verarbeitung Verantwortlichen“, dem Verantwortlichen allgemein die Einhaltung der DSGVO auferlegen. Allerdings verpflichtet Art. 24 Abs. 1 DSGVO den

[45] Dies widerspricht aber gerade den Änderungen im Gesetzgebungsprozess: Paal/Pauly/*Frenzel*, Art. 5 DSGVO, Rn. 50. Kritisch insgesamt: G/S/S/V/*Buchholtz/Stentzel*, Art. 5 DSGVO, Rn. 42 ff.

[46] Dies ergibt sich a. aus dem Titel von Art. 6 DSGVO: „Rechtmäßigkeit der Verarbeitung“.

[47] So für die DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12; *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 33.

[48] Ehmann/Selmayr/*Heberlein*, Art. 5 DS-GVO, Rn. 6.

Verantwortlichen nur zu geeigneten technischen und organisatorischen Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Auch hiermit geht keine Globalverpflichtung des Verantwortlichen im Sinne eines persönlichen Anwendungsbereichs einher.

Eine solch globale Verpflichtung widerspricht auch der Regelungssystematik der DSGVO. Der Verantwortliche wird als Normadressat regelmäßig entweder direkt oder indirekt per Normverweis angesprochen.[49] Bestes Beispiel hierfür sind die Befugnisse der Aufsichtsbehörde in Art. 58 DSGVO. Dort wird der Verantwortliche in nahezu jeder Befugnis explizit als Adressat aufgeführt. Aber auch abseits der Befugnisse der Aufsichtsbehörden finden sich Pflichten, die spezifisch dem Verantwortlichen, teilweise auch dem Auftragsverarbeiter zugewiesen werden. Dies gilt etwa für das Verfahrensverzeichnis nach Art. 30 DSGVO, die Sicherheit der Verarbeitung nach Art. 32 DSGVO, die Datenschutzfolgeabschätzung nach Art. 35 DSGVO und die Benennung eines Datenschutzbeauftragten nach Art. 37 DSGVO. Sämtliche dieser Pflichten finden sich im Kapitel IV „Verantwortlicher und Auftragsverarbeiter", dessen Abschnitt 1 mit „Allgemeine Pflichten" betitelt ist.

All dies spricht für eine normspezifische und nicht globale Zuweisung der Verantwortung des Verantwortlichen.[50] Sofern die Einhaltung einer Pflicht in einer Norm nicht explizit dem Verantwortlichen zugewiesen wird, sollte daher der erste Schluss nicht sein, dessen Verantwortlichkeit trotzdem kraft Systematik herzuleiten,[51] sondern die fehlende Zuweisung zu hinterfragen.[52] Das Erfordernis einer expliziten Zuweisung der Verantwortlichkeit steht auch nicht im Widerspruch dazu, dass der Verantwortliche in einer Vielzahl von Normen tatsächlich der Adressat ist.[53] Diese Normen beinhalten die Grundsätze der Verarbeitung nach Art. 5 DSGVO, die

[49] Vgl. etwa für Art. 83 Abs. 5 DSGVO: Simitis/Hornung/Spiecker/*Boehm*, Art. 83 DSGVO, Rn. 47.

[50] So etwa Ehmann/Selmayr/*Heberlein*, Art. 5 DS-GVO, Rn. 5, 39 für Art. 5 Abs. 2 DSGVO. Dieser betont vielmehr den Nachweisbarkeitsaspekt ggü. Aufsichtsbehörden im Rahmen der Rechenschaftspflicht.

[51] So etwa: G/S/S/V/*Kramer*, Art. 4 Nr. 7 DSGVO, Rn. 2.

[52] Anders die Art. 29-Datenschutzgruppe für die Zuweisung der Pflichten in der DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5. Widersprüchlich dazu: ebd., 7.

[53] So stellt etwa *Alsenoy*, CLSR[28] (2012), 25, 25 zur DSRL fest: „[...] the controller is the entity that carries primary responsibility for ensuring compliance with the substantive provisions [...]". Ähnlich a.: *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 20; Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 5 f. Siehe a. die Übersichtstabelle bei: S/J/T/K/*Schwartmann/Mühlenbeck*, Art. 4 DSGVO, Rn. 170.

Erfüllung der Betroffenenrechte nach Art. 12 ff. DSGVO, die spezifischen Pflichten nach Art. 24 ff. DSGVO, die Mehrheit der aufsichtsbehördlichen Befugnisse nach Art. 58 DSGVO, die Rechtsbehelfe sowie Schadensersatz und Geldbuße nach Art. 77 ff. DSGVO. In all diesen Fällen erfolgt die Zuweisung der Verantwortlichkeit an den Verantwortlichen aber ausdrücklich.[54] Den Verantwortlichen treffen somit zwar die meisten Pflichten der DSGVO,[55] allerdings nicht notwendigerweise alle.[56]

Versteht man das Datenschutzrecht zudem, jedenfalls in Teilen, als besonderes Gefahrenabwehrrecht,[57] ist die Bestimmung des Normadressaten, entsprechend dem Pflichtigen im allgemeinen Polizei- und Ordnungsrecht, einer der zentralen Punkte. Dies gilt jedenfalls soweit, wie die Maßnahmenbefugnisse der Aufsichtsbehörde nicht bereits selbst Adressaten benennen. Denn gegenüber demjenigen, dem eine konkrete Pflicht auferlegt wird, können die Aufsichtsbehörden auch Maßnahmen ergreifen. Im deutschen Recht enthalten sowohl das allgemeine Polizei- und Ordnungsrecht[58] wie auch das Baurecht[59] als besonderes Ordnungsrecht ausdifferenzierte Regelungen zu den Adressaten von Maßnahmen. In § 4 Abs. 1 POG RLP heißt es etwa: „Verursacht eine Person eine Gefahr, so sind die Maßnahmen gegen sie zu richten." Neben diesem Verhaltensstörer gibt es auch noch den Zustandsstörer gem. § 5 POG RLP. Diese allgemeinen Festlegungen der möglichen Adressaten schließen zwar nicht aus, dass spezifische Maßnahmen den konkreten Adressaten abweichend bestimmen, allerdings folgt daraus eine Regel-Ausnahme-Systematik. Soweit kein Adressat in einer konkreten Maßnahme benannt wird, kann die Polizei oder Bauaufsicht auf die allgemeine Adressatenfestlegung in §§ 4 oder 5 POG RLP zurückgreifen. Solch eine Regel-Ausnahme-Systematik findet sich ebenso, wenn die Polizei oder Bauaufsicht eine nicht verantwortliche Person in Anspruch nehmen will. Eine vergleichbare Regel-Ausnahme-Systematik findet man in der DSGVO hingegen nicht. In der DSGVO wird, wie bereits dargestellt, kein Adressat allgemein festgelegt. Auch für die Befugnisse der Aufsichtsbehörde gem. Art. 58 DSGVO wird kein allgemeiner Adressat normiert. Der Verantwortliche wird legaldefiniert, ohne dass er allgemein als Adressat der

[54] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 4. Vgl. zur eingeschränkten Relevanz im Übereinkommen Nr. 108 des Europarates: ebd., 5, 10.

[55] Nachdrücklich: *Monreal*, CR 2019, 797, Rn. 23 („Der Verantwortliche ist der primäre Normadressat der DSGVO."). Ähnlich: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 1 für die DSRL.

[56] Für die DSRL: Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 11.

[57] Dazu: Kapitel 5 K. I. Aufsichtsbehördliche Maßnahmen als Gefahrenabwehrrecht.

[58] Etwa §§ 4 ff. POG RLP.

[59] §§ 54 ff. LBauO RLP. Die Verantwortlichen werden zudem durch den Verweis auf das allgemeine Polizei- und Ordnungsrecht anhand von § 59 Abs. 2 LBauO RLP i.V.m. § 7 POG RLP ergänzt.

DSGVO erkennbar ist. Die Festlegung des jeweiligen Adressaten erfolgt vielmehr im Rahmen der konkreten Pflichten.

2. Der Verantwortliche im Kontext zentraler Fragen der DSGVO

Abseits dessen, dass ein Adressat für die DSGVO allgemein normiert wird, lässt sich erwägen, ob ein allgemeiner Adressat zumindest immanent aus der Systematik der DSGVO hergeleitet werden kann. Wäre also beispielsweise der Verantwortliche wiederum für andere zentrale Fragen der DSGVO, wie etwa den räumlichen Anwendungsbereich oder die Zuständigkeit der Aufsichtsbehörde maßgeblich, könnte damit auf eine systematische Herleitung eines allgemeinen Adressaten der DSGVO geschlossen werden. Dabei müsste allerdings auch berücksichtigt werden, ob die Bedeutung des Verantwortlichen wiederum in den Normen, in denen er explizit erwähnt wird, im Rahmen von anderweitigen Voraussetzungen eingeschränkt wird. Dies könnte etwa für die Bemessung der Geldbuße nach Art. 83 DSGVO gelten. Inwiefern der Verantwortliche maßgeblich für andere zentrale Fragen der DSGVO ist, soll Gegenstand der folgenden Analyse sein.

a) Der Verantwortliche und der räumliche Anwendungsbereich

Für die Eröffnung des räumlichen Anwendungsbereichs der DSGVO gibt es in Art. 3 drei verschiedene Möglichkeiten.[60] Diese knüpfen grob an

- die Niederlassung eines Verantwortlichen (oder Auftragsverarbeiters) in der Union,
- das Angebot von Waren oder Dienstleistungen an betroffene Personen in der Union,
- die Beobachtung des Verhaltens von betroffenen Personen in der Union und
- die Anwendbarkeit mitgliedstaatlichen Rechts durch Völkerrecht an.

Dabei muss bei der Erwähnung der Union auch immer der Europäische Wirtschaftsraum (EWR) mitgedacht werden.[61]

[60] Zu weiteren denkbaren Anknüpfungsmöglichkeiten: *Burkert*, 2.3 Internationale Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 7.

[61] Zur Geltung der DSGVO für den EWR: Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society)

aa) Niederlassungsprinzip

Zum einen soll die DSGVO gem. Art. 3 Abs. 1 dann anwendbar sein, wenn im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen (oder eines Auftragsverarbeiters) in der Union eine Verarbeitung personenbezogener Daten erfolgt, unabhängig davon, ob die Verarbeitung selbst in der Union (oder dem EWR) stattfindet.[62] Vorliegen müssen also:

- eine Verarbeitung personenbezogener Daten, unabhängig davon, ob die Verarbeitung in der Union erfolgt,
- ein über diese Verarbeitung bestimmbarer Verantwortlicher (oder Auftragsverarbeiter), der eine Niederlassung im Gebiet der Union hat,
- eine Verarbeitung im Rahmen der Tätigkeiten dieser Niederlassung.

Bezeichnet wird dieser Ansatz als Niederlassungsprinzip.[63] Über das Tatbestandsmerkmal „im Rahmen der Tätigkeit" wird die Verarbeitung grob dem Tätigkeitsfeld des Verantwortlichen zugeordnet, potenziell mit dem Ausschluss atypischer Verarbeitungen.[64] In den Rahmen der Tätigkeit fällt jedenfalls die eigene technische Vornahme der Verarbeitung oder deren maßgebliche Steuerung.[65] Ebenso reicht auch eine untrennbare Verknüpfung der Tätigkeit der Niederlassung mit derjenigen Niederlassung, die die Verarbeitung vornimmt, aus.[66] Was konstituiert nun eine Niederlassung? Wie sich aus ErwGr 22 S. 2 DSGVO ergibt, setzt eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus.[67] Nach ErwGr 22 S. 3 DSGVO ist die Rechtsform der Niederlassung unerheblich. Es werden sowohl Zweigstellen wie auch

and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022].

[62] Die Norm wird ergänzt durch ErwGr 22 DSGVO. Das mitgliedstaatliche Äquivalent für Deutschland findet sich in § 1 Abs. 4 S. 2 Nr. 2 BDSG.

[63] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 18.

[64] Was „im Rahmen der Tätigkeit" bedeutet wird nicht wirklich klar, die Rechtsprechung zu EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 55 ff. scheint jedenfalls nur eingeschränkt übertragbar: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 28 ff. Unerheblich ist diese Frage aber keinesfalls, vgl. ebd., Rn. 45.

[65] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 26.

[66] A. nach Einführung des Marktortprinzips: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 31.

[67] *Golland*, DuD 2018, 351, 353 macht anhand dessen die „gewisse Beständigkeit einer festen Einrichtung" (Einrichtungs-Element) und die „effektive Ausübung von Tätigkeiten im Mitgliedstaat" (Tätigkeits-Element) als Definitionsmerkmale aus.

Tochtergesellschaften mit eigener Rechtspersönlichkeit erfasst.[68] Dabei wird letztlich eine Bindung der Muttergesellschaft an datenschutzrechtliche Pflichten begründet, die gerade bei mehreren Tochtergesellschaften/Niederlassungen zu Problemen führen kann.[69] Daneben ist ein Unternehmenssitz auch nicht notwendigerweise eine Niederlassung.[70] Überhaupt scheint der Begriff „Niederlassung“[71] und „niedergelassen“ unglücklich gewählt.[72] Denn auch Privatpersonen sollen, sofern sie nicht unter die sogenannte Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO fallen, von der DSGVO erfasst werden. Folglich muss der Begriff der Niederlassung weit als Wohnsitz bzw. gewöhnlicher Aufenthaltsort für natürliche Personen ausgelegt werden.[73] Dabei ergeben sich aber offensichtliche Brüche mit den Definitionsmerkmalen aus ErwGr 22 S. 2 DSGVO. Dieses weite Verständnis deckt sich zudem nicht systematisch mit dem Begriff der Niederlassung aus der Niederlassungsfreiheit in Art. 49 AEUV.[74]

Inwiefern finden sich im Niederlassungsprinzip nun Anklänge zum Konzept der Verantwortlichkeit? Das Niederlassungsprinzip setzt im Rahmen des Tatbestandsmerkmals der Niederlassung zunächst weder eine juristische noch eine natürliche Person – im Gegensatz zum Verantwortlichen – voraus. Bei der Niederlassung wird überhaupt nicht auf ein Subjekt, wie eine Person, abgestellt, sondern auf ein Objekt, nämlich eine feste Einrichtung. Auch hinsichtlich der effektiven und tatsächlichen Ausübung einer Tätigkeit finden sich keine Anklänge an eine Entscheidung über die Verarbeitung, so wie sie die Definition des Verantwortlichen voraussetzt.

Das Niederlassungsprinzip basiert vielmehr auf einer organisatorischen Annäherung an den Verantwortlichen, oder auch den Auftragsverarbeiter, anhand einer Niederlassung.[75] Die Niederlassung kann dem Verantwortlichen organisatorisch zugeordnet werden, sie steht aber weder mit der Verarbeitung oder der Entscheidung

[68] Zur Figur der Scheinniederlassung: *Golland*, DuD 2018, 351, 353 f.

[69] Insb. hinsichtlich verschiedener Mitgliedstaaten: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 35 ff.

[70] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 18; Vgl. zur DSRL: EuGH, Urteil vom 01.10.2015 – C-230/14 (Weltimmo) = ZD 2015, 580, Rn. 29. Ebenso ist a. der Auftragsverarbeiter keine Niederlassung: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 33.

[71] Vergleichbar die englische Version mit „establishment“ und „established“ sowie die französische Version mit „établissement“ und „établi“.

[72] Kritisch: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 25.

[73] So a. *Golland*, DuD 2018, 351, 355 mit Verweis auf Grüneberg/*Thorn*, Art. 19 Rom I, Rn. 1, 5 f.

[74] Grabitz/Hilf/Nettesheim[81]/*Forsthoff*, Art. 49 AEUV, Rn. 16.

[75] Zu Umsetzungsproblemen der Vorgängerregelung der DSRL: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 6; Auernhammer/*Lewinski*, § 1 BDSG a.F., Rn. 50.

hierüber notwendigerweise in engem Bezug.[76] Die Verarbeitung selbst muss gar nicht in der Union stattfinden. Auffällig ist hierbei, dass der räumliche Anwendungsbereich im Rahmen des Niederlassungsprinzips weder direkt über den Ort der Verarbeitung[77] noch über den Ort der Entscheidung des Verantwortlichen über die Verarbeitung hergeleitet wird.[78] Der Ort der Verarbeitung ist bereits vom Normtext ausgehend irrelevant,[79] ein Bezug zum Ort der Entscheidung nicht ersichtlich.[80]

Zentraler Anknüpfungspunkt für den räumlichen Anwendungsbereich im Falle des Niederlassungsprinzips ist also ein räumlicher Bezug des Verantwortlichen zur Union anhand der Niederlassung. Entscheidend für diesen räumlichen Bezug ist nicht eine technische (die Verarbeitung) oder organisatorische (die Entscheidung über die Verarbeitung) Handlung, sondern ein allgemeiner Konnex (im Rahmen der Tätigkeit) der Verarbeitung zur Union. Allerdings muss dieser Konnex nicht einmal zwingend durch den Verantwortlichen vermittelt werden, da der räumliche Anwendungsbereich bei Art. 3 Abs. 1 DSGVO für den Verantwortlichen und den Auftragsverarbeiter separat zu bestimmen ist.[81] Das Niederlassungsprinzip hat durch diese Voraussetzung eines allgemeinen Konnexes über die Niederlassung den Vorteil eines weiten Anwendungsbereichs. Dass der Verantwortliche maßgeblich für den räumlichen Anwendungsbereich im Rahmen des Niederlassungsprinzips ist, lässt sich insgesamt allerdings nicht erkennen.

bb) Marktortprinzip

Daneben findet die DSGVO gem. Art. 3 Abs. 2 Anwendung auf einen nicht in der Union niedergelassenen Verantwortlichen (oder Auftragsverarbeiter), wenn die Verarbeitung personenbezogener Daten von betroffenen Personen in der Union entweder im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen in der Union (unabhängig von deren Kostenpflichtigkeit) oder im Zusammenhang mit

[76] So geht es nicht etwa um den Hauptsitz des Verantwortlichen. Vgl. zur DSRL: Dammann/Simitis DSRL/*Dammann*, Art. 4, Rn. 2 f.

[77] Auf diesen nimmt etwa § 1 Abs. 4 S. 2 Nr. 1 BDSG für den mitgliedstaatlichen Anwendungsbereich Bezug. Mit berechtigter Kritik an diesem Ansatz: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 27.

[78] Vgl. zu Überlegungen im Gesetzgebungsprozess der DSRL: *Caspar*, DuD 2015, 589, 591.

[79] Vgl. für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Vorbem. DSRL, Rn. 59; *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 15, 23.

[80] Im Gegenteil, nach EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 63 ist der eigentliche Entscheidungsort für die Frage der Zuständigkeit (die indirekt mit dem Anwendungsbereich zusammenhängt, vgl. ebd., Rn. 61) unerheblich.

[81] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 32.

der Beobachtung des Verhaltens von betroffenen Personen in der Union steht.[82] Voraussetzungen sind also:

- die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich im Gebiet der Union befinden,
- durch einen nicht in der Union niedergelassenen Verantwortlichen (oder Auftragsverarbeiter),
- ein Zusammenhang der Verarbeitung mit
    - dem Angebot von Waren oder Dienstleistungen in der Union (unabhängig von einer Kostenpflichtigkeit) oder
    - der Beobachtung des Verhaltens von betroffenen Personen in der Union.

Bezeichnet wird dieser Ansatz als Marktortprinzip. In Abgrenzung zum Niederlassungsprinzip werden mit diesem Ansatz Verarbeitungen erfasst, die sich zwar auf das Gebiet der Union beziehen, allerdings von einem nicht in der Union niedergelassenen Verantwortlichen durchgeführt werden. Da es sich um einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter handeln muss, ist das Niederlassungsprinzip vorrangig zu prüfen.[83] Die vorrangige Prüfung des Niederlassungsprinzips ist auch deswegen erheblich, weil bei Anwendbarkeit des Marktortprinzips ein Vertreter gem. Art. 27 Abs. 1 DSGVO durch den Verantwortlichen oder Auftragsverarbeiter zu bestellen ist.[84] Unklar ist hinsichtlich des Marktortprinzips, ob und gegebenenfalls wie das Niedergelassensein[85] in Art. 3 Abs. 2 DSGVO vom in Art. 3 Abs. 1 DSGVO verwendeten Begriff der Niederlassung abzugrenzen ist.[86]

Angeknüpft wird beim Marktortprinzip wiederum nicht an eines der Definitionselemente des Verantwortlichen. Stattdessen ist zum einen eine objektiv erkennbare Absicht des Verantwortlichen maßgeblich, nämlich das Angebot von

[82] Die deutsche Entsprechung, die allerdings völlig unklar lässt, wo der spezifische Bezug zu Deutschland liegen soll, findet sich in § 1 Abs. 4 S. 2 Nr. 3 BDSG (dazu: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 15 f., 64).

[83] So etwa: *Golland*, DuD 2018, 351, 352. Zu Abgrenzungsschwierigkeiten: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 44 f.

[84] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 31.

[85] Im Wortlaut „niedergelassenen".

[86] Dies gilt a. für Art. 3 Abs. 3 DSGVO. *Golland*, DuD 2018, 351, 352 will das „niedergelassen" aus Abs. 2 und 3 deckungsgleich mit der Niederlassung aus Abs. 1 verstehen, einschließlich des Merkmals „im Rahmen der Tätigkeit".

Waren oder Dienstleistungen.[87] Zum anderen wird an das faktische, also nicht nur das beabsichtigte, Beobachten des Verhaltens von betroffenen Personen in der Union angeknüpft.[88] Diese Anknüpfungspunkte müssen allerdings nicht Zweck der Verarbeitung sein. Ein im Zusammenhang stehen reicht aus. Somit besteht auch kein besonderer Bezug zur Entscheidung des Verantwortlichen über die Zwecke, die Teil der Definition des Verantwortlichen ist. Wie bei Abs. 1 ist auch bei Art. 3 Abs. 2 DSGVO der Ort der Verarbeitung unerheblich.[89] Ebenso ist bei Art. 3 Abs. 2 DSGVO die Anwendbarkeit jeweils für den Verantwortlichen und den Auftragsverarbeiter separat zu bestimmen. Festhalten lässt sich somit für das Marktortprinzip, dass zentraler Anknüpfungspunkt hier die Ausrichtung bestimmter, im Zusammenhang mit der Verarbeitung stehender, Tätigkeiten auf die Union ist; Anknüpfungspunkt ist hingegen nicht der Verantwortliche oder dessen Entscheidung über die Verarbeitung. Es wäre demnach denkbar nur durch die Verarbeitung die räumliche Anwendbarkeit zu bestimmen, also ohne überhaupt den Verantwortlichen zu kennen.

cc) Via Völkerrecht

Als letzte Möglichkeit sieht Art. 3 Abs. 3 DSGVO die Anwendung der DSGVO dann vor, wenn der Verantwortliche an einem Ort niedergelassen ist, der zwar nicht in der Union liegt, aufgrund von Völkerrecht allerdings dem Recht eines Mitgliedstaates der Union unterliegt.[90] Gem. ErwGr 25 DSGVO sollen damit insbesondere diplomatische und konsularische Vertretungen erfasst werden.[91] Aufgrund des Begriffs „niedergelassen" dürften allerdings nur nicht-öffentliche Verantwortliche erfasst sein. Dies schränkt den Anwendungsbereich deutlich ein.[92] Denkbar ist die Anwendung vor allem in Flugzeugen oder Schiffen aufgrund des Flaggenprinzips.[93] Allerdings stellt sich dabei die Frage, inwiefern ein Verantwortlicher dort überhaupt niedergelassen ist.

[87] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 50; siehe a. ErwGr 23 S. 2 DSGVO.
[88] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 61; siehe a. ErwGr 24 DSGVO.
[89] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 46.
[90] Zur missverständlichen deutschen Version: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 67.
[91] Dammann/Simitis DSRL/*Dammann*, Art. 4, Rn. 5 vertieft dies im Rahmen der DSRL nicht weiter, stellt aber klar, dass das Recht des Gaststaates nur zurücktritt. Ebenso: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 4 DSRL, Rn. 16.
[92] Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 66.
[93] Dort allerdings a. nur außerhalb des Luft- bzw. Seegebiets von Staaten, wenn also das Flaggenprinzip Anwendung findet.

Daneben ist systematisch nicht nachvollziehbar, warum der Auftragsverarbeiter in Art. 3 Abs. 3 DSGVO keine Erwähnung findet.[94]

Bezugspunkt bei der Anwendung aufgrund von Völkerrecht ist das Niedergelassensein des Verantwortlichen an einem bestimmten Ort. Art. 3 Abs. 3 DSGVO unterscheidet sich von Art. 3 Abs. 1 DSGVO nur dadurch, wie die Anwendbarkeit des mitgliedstaatlichen Rechts begründet wird. Sie wird eben nicht territorial, sondern durch Völkerrecht begründet. Insofern gelten für Art. 3 Abs. 3 DSGVO die gleichen Erwägungen wie beim Niederlassungsprinzip nach Art. 3 Abs. 1 DSGVO.

dd) Zwischenfazit

Bei allen drei Varianten der Eröffnung des räumlichen Anwendungsbereichs der DSGVO findet sich kein Anknüpfungspunkt, der direkt auf den Verantwortlichen oder seine Definitionselemente Bezug nimmt. Der Verantwortliche wird nur soweit in Bezug genommen, wie er in der Union niedergelassen ist oder eben nicht. Beim Marktortprinzip scheint sogar der Fokus eher noch auf dem Kontext der Verarbeitung als entscheidendem Kriterium zu liegen. Bei der Feststellung des räumlichen Anwendungsbereichs zeigt sich, dass der Verantwortliche hierfür zwar ein Bezugspunkt ist, er ist aber eben nicht zentrales Kriterium hierfür.[95] Dies bestätigt auch die rechtshistorische Perspektive, da ursprünglich der Ort der Datei maßgeblich für das anwendbare Recht sein sollte.[96] Dieser Ansatz wurde wegen Schwierigkeiten bei der Bestimmung dieses Ortes allerdings verworfen.[97]

b) Der Verantwortliche und die Zuständigkeit der Aufsichtsbehörde

Die Zuständigkeit der Aufsichtsbehörde bestimmt sich unabhängig vom räumlichen Anwendungsbereich nach Art. 55 DSGVO. Maßgeblich ist hierbei Art. 55 Abs. 1 DSGVO. Demnach ist die Aufsichtsbehörde im Hoheitsgebiet ihres eigenen Mitgliedstaats für die Erfüllung der Aufgaben und die Ausübung der Befugnisse gemäß der DSGVO zuständig. Dieser Ansatz wird als Territorialitätsprinzip bezeichnet.[98]

[94] So a.: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 68.

[95] So wohl a.: *Lewinski/Herrmann*, ZD 2016, 467, 469 f., anders für die DSRL wohl: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 18 und Grabitz/Hilf[40]/*Brühann*, A 30 Art. 4 DSRL, Rn. 11 f. Die DSRL enthielt in ErwGr 21 noch die Feststellung, dass die im Strafrecht geltenden Territorialitätsregeln unberührt bleiben.

[96] Für die DSRL: BT-Drs. 12/8329, S. 16; vgl. Dammann/Simitis DSRL/*Dammann*, Art. 4, Rn. 2 f.

[97] BT-Drs. 12/8329, S. 16; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 4 DSRL, Rn. 4 ff.

[98] Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 1.

Art. 55 Abs. 2 DSGVO legt zudem fest, dass bei einer Verarbeitung durch eine Behörde oder private Stelle nach Art. 6 Abs. 1 lit. c oder e DSGVO die Aufsichtsbehörde des betroffenen Mitgliedstaats zuständig ist. Damit wird vor allem eine Ausnahme von der Zuständigkeit der federführenden Aufsichtsbehörde nach Art. 56 DSGVO geschaffen.[99]

Art. 55 Abs. 1 DSGVO regelt also zwar die räumlichen Grenzen der aufsichtsbehördlichen Befugnisse, nicht aber deren Voraussetzungen. Ein Rückgriff auf Art. 3 DSGVO ist weder möglich noch zielführend, da dort nur der räumliche Anwendungsbereich der DSGVO allgemein geregelt wird.[100] Die Frage, wann die Aufsichtsbehörde welches Mitgliedstaats gegen einen Verantwortlichen vorgehen kann oder wann welches mitgliedstaatliches Recht anwendbar ist, wird damit nicht geklärt. Weitere Details zur Zuständigkeit der Aufsichtsbehörde erschließen sich erst aus ErwGr 122 S. 2 DSGVO. Demnach soll eine Aufsichtsbehörde insbesondere zuständig sein für

- die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen (oder Auftragsverarbeiters) im Hoheitsgebiet des jeweiligen Mitgliedstaats,
- die Verarbeitung personenbezogener Daten durch Behörden oder private Stellen, die im öffentlichen Interesse handeln,
- Verarbeitungstätigkeiten, die Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet haben oder
- für Verarbeitungstätigkeiten eines Verantwortlichen oder Auftragsverarbeiters ohne Niederlassung in der Union, sofern sie auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet ausgerichtet sind.[101]

Nach Art. 55 Abs. 1 DSGVO können die Anwendung mitgliedstaatlichen Rechts und die Ausübung der aufsichtsbehördlichen Befugnisse durchaus auseinanderfallen.[102] Dies dürfte insbesondere für Verarbeitungstätigkeiten gelten, die

[99] Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 1, 18. Siehe a. ErwGr 128 DSGVO.
[100] Vgl. Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 6.
[101] Zu Folgeproblemen: Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 14 ff.
[102] Noch zur DSRL: *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 47; EuGH, Urteil vom 01.10.2015 – C-230/14 (Weltimmo) = ZD 2015, 580, Rn. 54 ff.; Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 5, 9.

Auswirkungen auf betroffene Personen im jeweiligen Hoheitsgebiet haben.[103]

Ähnlich wie beim räumlichen Anwendungsbereich ist auch bei der Frage der Zuständigkeit der Aufsichtsbehörde kein maßgeblicher Bezug zum Verantwortlichen oder wenigstens zu einem seiner Definitionselemente erkennbar. Hinsichtlich der Zuständigkeit für Verarbeitungen im Rahmen der Tätigkeit der Niederlassung eines Verantwortlichen im Hoheitsgebiet eines bestimmten Mitgliedstaates gelten die Ausführungen zum Niederlassungsprinzip entsprechend.[104] Auch bei der Verarbeitung durch Behörden oder private Stellen[105], die im öffentlichen Interesse handeln, ist der Anknüpfungspunkt vor allem das Handeln im öffentlichen Interesse. Bei Verarbeitungstätigkeiten schließlich, die entweder Auswirkungen auf betroffene Personen im Hoheitsgebiet haben oder auf betroffene Personen mit Wohnsitz im Hoheitsgebiet ausgerichtet sind, ist der Anknüpfungspunkt die Absicht bei der Verarbeitung bzw. die Folgen der Verarbeitung. Damit ist vor allem der Kontext einer Verarbeitung für die Zuständigkeit der Aufsichtsbehörde relevant, nicht der Verantwortliche.

Der ursprüngliche Entwurf der Europäischen Kommission („Kommission") zur DSGVO sah demgegenüber noch eine Anknüpfung der Zuständigkeit der Aufsichtsbehörde an die Hauptniederlassung des Verantwortlichen vor. Mit diesem Bezug zur Hauptniederlassung hätte eine erkennbare Verbindung zwischen der Zuständigkeit der Aufsichtsbehörde und dem Verantwortlichen bestanden.[106] Denn bei der Hauptniederlassung eines Verantwortlichen liegt es nahe, dass diese auch über die Verarbeitung entscheidet. Im Gesetzgebungsprozess wurde der Ansatz über die Hauptniederlassung allerdings nicht weiterverfolgt, damit betroffene Personen ihre Rechte auch gegenüber Aufsichtsbehörden in den jeweiligen Heimatstaaten geltend machen konnten.[107]

Die Niederlassung als Kriterium für die Anwendbarkeit der DSGVO wie auch für die Zuständigkeit der Aufsichtsbehörde deckt sich insgesamt allerdings nicht unbedingt mit dem Konzept des Verantwortlichen. Denn bei einer Niederlassung handelt es sich nicht zwangsläufig um die Niederlassung des Verantwortlichen, die auch über die Verarbeitung entscheidet. Die Niederlassung als Konzept dient vielmehr

[103] Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 13.

[104] Dazu: Kapitel 1 A. II. 2. a) aa) Niederlassungsprinzip.

[105] Bei diesen müsste es sich strenggenommen nicht einmal um Stellen handeln, die im betreffenden Mitgliedstaat niedergelassen sind.

[106] Vgl. aber die Erwägungen zur innerdeutschen Zuständigkeit durch § 3 Abs. 1 Nr. 2 VwVfG anhand der Betriebsstätte: Kühling/Buchner/*Boehm*, Art. 55 DS-GVO, Rn. 17.

[107] Simitis/Hornung/Spiecker/*Polenz*, Art. 55 DSGVO, Rn. 3.

dazu, den Zugriff des jeweiligen Rechts und der Aufsichtsbehörde auf den Verantwortlichen zu ermöglichen. Deutlich wird dies im Urteil des EuGH in Wirtschaftsakademie.[108] Dort hatte der EuGH entschieden, dass ein Sitz des Verantwortlichen außerhalb der Union nichts an der Zuständigkeit der Aufsichtsbehörde aufgrund einer Niederlassung dieses Verantwortlichen ändert.[109]

c) Der Verantwortliche im Bußgeldverfahren und der funktionale Unternehmensbegriff aus dem Unionskartellrecht

Erkennbare Abweichungen vom Konzept des Verantwortlichen finden sich auch bei der Bemessung der Geldbuße gem. Art. 83 Abs. 4-6 DSGVO. Dabei geht es um den Begriff des Unternehmens. Dies wird vertieft im Rahmen der Folgen der Verantwortlichkeit unter dem Thema Geldbußen[110] behandelt.

3. Fazit

Deutlich wird anhand dieser Analyse, dass der Verantwortliche weder aufgrund der ihm zugeschriebenen Pflichten und Verantwortung noch aufgrund seiner Bedeutung für zentrale Fragen der DSGVO als allgemeiner Adressat der DSGVO verstanden werden kann. Die vielfältigen Pflichten des Verantwortlichen kommen nicht einer Festlegung des Verantwortlichen als allgemeinem Adressaten der DSGVO gleich. Der Verantwortliche dient als Zuordnungssubjekt für Verantwortung und ist im Rahmen dessen für die Einhaltung der wesentlichen, aber eben nicht aller Verpflichtungen der DSGVO zuständig.[111] Auch anhand der Kriterien für die räumliche Anwendbarkeit der DSGVO und die Zuständigkeit der Aufsichtsbehörde wird deutlich, dass das Konzept der Verantwortlichkeit keine maßgebliche Rolle hinsichtlich anderer zentraler Fragen der DSGVO spielt.

Daher lässt sich aus der Systematik der DSGVO auch nicht indirekt eine Stellung des Verantwortlichen als allgemeinem Adressaten der DSGVO ableiten.[112] Das dominierende Konzept der DSGVO ist vielmehr, wie es sich auch aus dem sachlichen Anwendungsbereich in Art. 2 Abs. 1 DSGVO ergibt, die Verarbeitung

[108] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.
[109] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 63.
[110] Dazu: Kapitel 3 C. I. Der funktionale Unternehmensbegriff als Maßstab.
[111] Vgl. Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 120; EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 35.
[112] Anders: *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 59 f.

(personenbezogener Daten).[113] Für diesen sachlichen Anwendungsbereich spielt der Verantwortliche wiederum keine Rolle. So wie sich der Verantwortliche anhand der Entscheidung über die Zwecke und Mittel der Verarbeitung über eben diese konstruiert,[114] so ist der Bezugspunkt für viele andere zentrale Fragen der DSGVO die Verarbeitung.[115]

B. Historische Entwicklung

Auch wenn es bereits vor 1970 erste Ansätze zum Datenschutz gab,[116] begann seine wesentliche Ausformung im Jahr 1970 mit dem Hessischen Datenschutzgesetz.[117] Eine Norm, die sich spezifisch mit einem allgemeinen datenschutzrechtlichen Adressaten beschäftigte, gab es trotz anderweitiger Konzepte, wie den Betroffenenrechten oder dem Datenschutzbeauftragten, noch nicht. Vielmehr wurden die Adressaten nur insofern bestimmt, als dass das Datenschutzrecht ausschließlich auf Behörden und öffentliche Stellen Anwendung fand. Die „speichernde Stelle" als Vorläufer des Verantwortlichen fand sich erst im ersten deutschen Bundesdatenschutzgesetz von 1977.[118] Sowohl der eingeschränkte Anwendungsbereich, die Fixierung auf den technischen Prozess der Speicherung (im BDSG 1977) wie auch die damals begrenzte Verfügbarkeit von Rechenleistung[119] illustrieren, dass zur Zeit der Genese des Datenschutzrechts Verarbeitungen praktisch nur in Großrechnern durch klar abgrenzbare Akteure wie Behörden oder Großunternehmen[120] durchgeführt

[113] Vgl. Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 58.

[114] Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 22.

[115] Dies galt bereits für die ersten Datenschutzgesetze: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 16. Vgl. für die DSRL: *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 18.

[116] So etwa der US-amerikanische Fair Credit Reporting Act (Inkrafttreten am 26.10.1970). Der US-Gesetzgeber verfolgte im Gegensatz zu den europäischen Staaten einen bereichsspezifischen bzw. sektoralen Ansatz: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 131 f. Detailliert: *Burkert*, 2.3 Internationale Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 78 ff.

[117] Vgl. *Hoffmann-Riem*, Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer/Micklitz/Tonner (Hrsg.), Law and diffuse Interests in the European Legal Order: Liber amicorum Norbert Reich, 1997, 778: „Geburtsstunde der gesetzlichen Verankerung des Datenschutzes". Detailliert: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 127 ff.

[118] Überblicksartig: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 2 ff.

[119] Dies war nicht nur technisch, sondern auch räumlich und finanziell, bedingt, wie der Begriff „Großrechner" verdeutlicht.

[120] Die nicht-öffentlichen Verantwortlichen wurden erst im BDSG 1977 erfasst.

wurden.[121] Das Datenschutzrecht war eine Art Sonderrecht, dass sich „außerhalb der Lebenswelt der Durchschnittsbürger vollzog".[122] Die Zuordnung der Verantwortlichkeit war anscheinend so offensichtlich,[123] dass sie zunächst gar nicht normiert werden musste. Auch die Reduktion der Verarbeitung auf bestimmte schutzwürdige Phasen[124] sowie der anfängliche Fokus auf die Datei als Schutzobjekt zeigt die Abhängigkeit des Datenschutzrechts von den technischen Bedingungen seiner Entstehungszeit. Die folgende Darstellung soll die Entwicklung des Datenschutzrechts im Hinblick auf den primären Adressaten von der „speichernden Stelle" über den „Verantwortlichen für die Datei" bis zum „Verantwortlichen" nach der DSGVO nachzeichnen.[125] Dabei werden neben der deutschen Entwicklung auch die europäischen und internationalen Bezüge hergestellt.[126] Den Abschluss bildet eine Analyse, ob das ursprüngliche Konzept des Adressaten trotz der technischen Entwicklung noch grundsätzlich anschlussfähig ist.[127]

I. HDSG (1970)

Das Hessische Datenschutzgesetz vom 7. Oktober 1970[128] gilt als das erste Datenschutzgesetz[129] weltweit.[130] Für eine Analyse der Entwicklung des Konzeptes des

[121] Vgl. a. *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 6.

[122] *Hoffmann-Riem*, Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer/Micklitz/Tonner (Hrsg.), Law and diffuse Interests in the European Legal Order: Liber amicorum Norbert Reich, 1997, 778.

[123] Vgl. Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 129 zum Grundton der Regelungen durch Generalklauseln.

[124] So etwa im BDSG 1977: speichern, übermitteln und verändern.

[125] Allgemein zur Geschichte des Datenschutzrechts bis 2003: *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003.

[126] Zu den beiden letzten Aspekten vgl. die Kommentierungen bei: Kuner/Bygrave/Docksey/Drechsler (Hrsg.), The EU General Data Protection Regulation (GDPR), 2020.

[127] Vgl. etwa *Hoffmann-Riem*, Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer/Micklitz/Tonner (Hrsg.), Law and diffuse Interests in the European Legal Order: Liber amicorum Norbert Reich, 1997, 779 grds. kritisch zur „Antiquiertheit des traditionellen Schutzkonzepts".

[128] Hessisches Datenschutzgesetz v. 07.10.1970, (hess.) GVBl. II 300-10, S. 625.

[129] Der Name scheint allein dahingehend berechtigt, dass nicht einmal ein Personenbezug vorliegen musste. Vgl. zum Begriff a. Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 2 f.; *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 12.

[130] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 1. Einen Überblick über die frühe deutsche Gesetzgebung enthält BT-Drs. 7/1027, S. 15 f. Auf internationaler Ebene: *Burkert*, 2.3 Internationale Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 14 ff.

Verantwortlichen ist ein Blick hierauf also unabdingbar. Denn dieses Gesetz legte das Fundament für die weitere Entwicklung des Datenschutzrechts. Der Verantwortliche wurde im HDSG 1970 selbst nicht definiert, er ergab sich aber insgesamt aus den Normen, die ihn verpflichteten. Dieses erste Datenschutzgesetz enthielt zudem einige bis heute vertraute Konzepte des Datenschutzrechts.[131] Diese Konzepte werden im Folgenden in Bezug zum Konzept des Verantwortlichen dargestellt. § 1 HDSG 1970 („Bereich des Datenschutzes") regelte zunächst den sachlichen[132] wie auch persönlichen Anwendungsbereich des Datenschutzes:

> *„Der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts."*

Man kann im zweiten Teil der Norm (*„[...] im Bereich des Landes [...]"*) auch eine Eingrenzung des sachlichen Anwendungsbereichs erkennen, allerdings bliebe dann die Frage offen, wer überhaupt durch die weiteren Normen verpflichtet würde. Die Notwendigkeit eines solchen Normadressaten wurde bereits in § 2 HDSG 1970 („Inhalt des Datenschutzes") deutlich, der Pflichten für den Umgang mit den vom Datenschutz erfassten Unterlagen, Daten und Ergebnissen festlegte:

> *„Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen."*

In dieser Vorschrift fanden sich auch erste Andeutungen auf die später in § 9 BDSG a.F. fixierten technischen und organisatorischen Maßnahmen (TOMs).[133]

In § 3 Abs. 1 HDSG 1970 („Datengeheimnis") war das Datengeheimnis verankert.

---

[131] Vgl. zu den Elementen: *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, ²2012, Rn. 88; *Roßnagel*, 1. Einleitung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 19.

[132] Vgl. für die DSGVO Art. 2 Abs. 1.

[133] Vgl. für die DSGVO Art. 32.

Demnach war es den mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung betrauten Personen untersagt, die dabei erlangten Kenntnisse über Unterlagen, Daten und Ergebnisse anderen mitzuteilen oder anderen zu gestatten oder sie dabei zu fördern, derartige Kenntnisse zu erlangen.[134] Ausnahmsweise war dies aber dann gestattet, wenn eine entsprechende Rechtsvorschrift oder die Zustimmung einer über die Unterlagen, Daten und Ergebnisse verfügungsberechtigten Person vorlag. Das Verbot galt nach § 3 Abs. 2 HDSG 1970 ebenso dann nicht, wenn diese Handlungen zur verwaltungsmäßigen oder technischen Durchführung der Datenverarbeitung erforderlich waren. Dieses Datengeheimnis findet sich in abgewandelter Form heute noch in Art. 29 DSGVO.[135] Durch den Kreis der dem Datengeheimnis Verpflichteten, insbesondere im Verhältnis untereinander, ließ sich bereits eine Eingrenzung der Normadressaten im HDSG 1970 vornehmen. Normadressaten von § 3 HDSG 1970 konnten dabei nur die in Art. 1 HDSG 1970 genannten Stellen sein.[136]

§ 4 HDSG 1970 („Anspruch auf Datenschutz") regelte die Berichtigungsmöglichkeit gespeicherter Daten durch den Betroffenen sowie, bei der Verletzung von § 2 S. 1 HDSG 1970, einen Anspruch auf Wiederherstellung des früheren Zustands und, bei Gefahr weiterer Verletzungen, auch einen Anspruch auf Unterlassung. Hier fanden sich also die ersten Anzeichen von Betroffenenrechten.[137] Auch für diese Ansprüche konnten nur die in § 1 HDSG 1970 genannten Stellen Normadressat sein.

Eine gewisse organisatorische Eingrenzung der Normadressaten ließ sich zudem § 5 Abs. 2 HDSG 1970 („Datenbanken und Informationssysteme") entnehmen. Demnach war zu gewährleisten:

> *„[…] daß keine Stellen Unterlagen, Daten und Ergebnisse einsehen oder abrufen können, die nicht auf Grund ihrer Zuständigkeiten hierzu befugt sind."*

Der Normadressat im HDSG 1970 ergab sich also im Zusammenspiel zwischen den in § 1 HDSG 1970 genannten Stellen sowie der entsprechenden Sachzuständigkeit. Daneben erlaubte § 5 Abs. 1 HDSG 1970 für den Aufbau von Datenbanken und Informationssystemen sowie für statistische Zwecke den in § 1 HDSG 1970 genannten

---

[134] Vgl. dazu Simitis/*Ehmann*, § 5 BDSG a.F., Rn. 15.

[135] Simitis/Hornung/Spiecker/*Petri*, Art. 29 DSGVO, Rn. 2 ff.

[136] Ebenso dürften diese Stellen identisch mit dem Begriff der verfügungsberechtigten Person gewesen sein.

[137] Vgl. für die DSGVO Art. 12 ff.

Stellen die Weitergabe von Unterlagen, Daten und Ergebnisse. Auch diese Ermächtigung ist ein Indiz dafür, dass die genannten Stellen die Normadressaten darstellten. Eine weitere Erwähnung der in § 1 HDSG 1970 genannten Stellen erfolgte in § 10 Abs. 1, § 11 sowie § 13 HDSG 1970.

Eine organisatorische Differenzierung zwischen verantwortungstragender Stelle und technisch durchführender Stelle schien durch § 6 HDSG 1970 impliziert. Demnach hatten der Landtag, der Präsident des Landtags sowie dessen Fraktionen nach § 6 Abs. 1 HDSG 1970, innerhalb ihrer Zuständigkeit, ein Auskunftsrecht gegenüber den verschiedenen Rechenzentren und Datenverarbeitungsanlagen. Entsprechendes galt gem. § 6 Abs. 2 HDSG 1970 für die Gemeindevertretungen, Kreistage, deren Fraktionen und die entsprechenden Organe der in § 1 HDSG 1970 genannten Körperschaften und Anstalten gegenüber Rechenzentren und Datenverarbeitungsanlagen. Der Datenschutz sollte die Unterlagen, Daten und Ergebnisse im Bereich der in § 1 HDSG 1970 genannten Stellen erfassen, gleichzeitig hatten aber die Organe dieser Stellen ein Auskunftsrecht gegenüber den Stellen, die die technische Verarbeitung durchführten, wie die Hessische Zentrale für Datenverarbeitung, die kommunalen Gebietsrechenzentren, die Landesbehörden sowie die Gemeinden und Landkreise, die Datenverarbeitungsanlagen betrieben.

§§ 7 ff. HDSG 1970 schließlich regelten den Datenschutzbeauftragten. Dieser bildete, wie § 10 Abs. 1 S. 2 HDSG 1970 zu entnehmen war, nicht selbst eine Aufsichtsbehörde, sondern er unterrichtete die jeweils zuständige Aufsichtsbehörde. Ungeachtet dessen bestand allerdings nach § 11 HDSG 1970 bereits ein Anrufungsrecht durch jedermann, wenn eine Person annahm, durch die maschinelle Datenverarbeitung der in § 1 genannten Stellen in ihren Rechten verletzt zu werden.[138] Dem Datenschutzbeauftragten selbst stand nach § 13 HDSG 1970 nur ein Auskunftsrecht gegenüber den in § 1 HDSG 1970 genannten Stellen zu. Eine Ordnungswidrigkeit bestand nach § 16 HDSG 1970 schließlich für den Fall, dass ein vorsätzlicher oder fahrlässiger Verstoß gegen § 3 HDSG 1970 vorlag.

Bereits im HDSG 1970 zeigte sich ein Dreiecksverhältnis zwischen betroffenen Personen, verpflichteten Stellen und Datenschutzbeauftragtem. Ebenso wurden die klassischen Rollen etabliert: der Verantwortliche, die betroffene Person und Dritte. Eine genaue Konturierung erfuhren diese verpflichteten bzw. verantwortungstragenden Stellen gleichwohl noch nicht. Deutlicher wurden diese

[138] Diese Norm könnte mitursächlich für das, teilweise heute noch bestehende, Verständnis von Datenschutzaufsichtsbehörden sein, dass es sich beim Beschwerderecht um eine Art Petitionsrecht handelt.

Stellen und ihre Pflichten mit der Reform des HDSG im Jahr 1978.[139] Zunächst wurde in § 3 Abs. 1 HDSG 1978 die Anwendbarkeit des Gesetzes ähnlich wie in § 1 HDSG 1970 für die entsprechenden Behörden und öffentlichen Stellen angeordnet. Allerdings enthielt § 2 Abs. 3 Nr. 1 HDSG 1978 eine Definition der speichernden Stelle, die auf § 3 Abs. 1 HDSG 1978 Bezug nahm:

> *„speichernde Stelle [ist] jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst speichert oder durch andere speichern lässt,"*

Die speichernde Stelle wurde im Zusammenhang mit der Definition des Speicherns in § 2 Abs. 2 Nr. 1 HDSG 1978 also technisch definiert. Die speichernde Stelle konnte aber auch durch andere speichern lassen.[140] Daneben wurde die Verantwortungssphäre der speichernden Stelle durch die Negativdefinition des Dritten in § 2 Abs. 3 Nr. 2 HDSG 1978 eingegrenzt. Auffällig ist im HDSG 1978 allerdings, dass die speichernde Stelle im Gesetz nicht regelmäßig als Normadressat verwendet wurde. Häufig wurde entweder auf die in § 3 Abs. 1 HDSG 1978 genannten Stellen Bezug genommen oder auf die überhaupt nicht definierten übermittelnden Stellen. Im HDSG 1986[141] wurde der Anwendungsbereich weiterhin identisch definiert.[142] Allerdings wurde nun in § 2 Abs. 3 HDSG 1986 statt der speichernden die datenverarbeitende Stelle definiert:

> *„Datenverarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt."*

Auch im HDSG 1986 wurde noch nicht einheitlich auf die datenverarbeitende Stelle als Normadressat Bezug genommen.

II. BDSG (1977)

Das erste Bundesdatenschutzgesetz[143] trat 1977 in Kraft.[144] Der Entwurf hierzu war allerdings bereits etwa dreieinhalb Jahre älter.[145] Der persönliche Anwendungsbereich

[139] Hessisches Datenschutzgesetz (HDSG) v. 31.01.1978, (hess.) GVBl. II 300-19, S. 96.
[140] Hiermit dürfte die Verarbeitung im Auftrag gem. § 4 HDSG 1978 gemeint sein.
[141] Hessisches Datenschutzgesetz (HDSG) v. 11.11.1986, (hess.) GVBl. II 300-28, S. 309.
[142] Zu den anderen Änderungen: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 50.
[143] Kritisch zum Begriff Datenschutz: BT-Drs. 7/1027, S. 14.
[144] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) v. 27.01.1977, BGBl. I Nr. 7 S. 201.
[145] BT-Drs. 7/1027.

erschloss sich aus § 1 Abs. 2 S. 1 BDSG 1977. Dieser unterschied drei verschiedene Arten von Normadressaten, die personenbezogene Daten in Dateien speicherten, veränderten, löschten oder aus Daten übermittelten:

- Behörden oder sonstige öffentliche Stellen,
- natürliche oder juristische Personen, Gesellschaften oder andere Personenvereinigungen des privaten Rechts für eigene Zwecke,
- natürliche oder juristische Personen, Gesellschaften oder andere Personenvereinigungen des privaten Rechts geschäftsmäßig für fremde Zwecke.

Der persönliche Anwendungsbereich dieser Adressaten wurde dann in den Normen, die den spezifischen Vorschriften für den jeweiligen Adressaten vorangingen, also § 7, § 22 und § 31 BDSG 1977, weiter vertieft. Daneben definierte § 2 Abs. 3 Nr. 1 BDSG 1977 die speichernde Stelle unter Verweis auf § 1 Abs. 2 S. 1 BDSG 1977 als

> *„speichernde Stelle [...], die Daten für sich selbst speichert oder durch andere speichern lässt,“.*[146]

Das „Speichern“ wiederum wurde in § 2 Abs. 1 Nr. 1 BDSG 1977 definiert als

> *„ [...] das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einen Datenträger zum Zwecke ihrer weiteren Verwendung,“*

Die Entwurfsfassung des BDSG aus dem Jahr 1973 enthielt noch keine Definition der speichernden Stelle.[147] Dieses Defizit hatte der Bundesrat in seiner Stellungnahme zum Entwurf angemahnt.[148] Irritierend ist hinsichtlich der Definition der speichernden Stelle, dass der Anwendungsbereich des BDSG 1977 mit der Veränderung, Übermittlung und Löschung in § 1 Abs. 2 eigentlich weiter als das bloße Speichern gefasst ist. Entsprechend musste also auch die speichernde Stelle als weiter gefasst

[146] Man kann die „speichernde Stelle“ also, jedenfalls nach deutschem Verständnis, a. als Oberbegriff für die spezifischen Adressaten verstehen: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 3.

[147] Ebenso wand sich der interparlamentarische Arbeitsgemeinschafts-Entwurf für ein BDSG an die Datenbanken des Bundes bzw. private Datenbanken (präziser an die Betreiber): BT-Drs. VI/2885, S. 1 f., 3 (§§ 4, 12).

[148] BT-Drs. 7/1027, S. 33. In Reaktion hierauf: BT-Drs. 7/5277, S. 6.

verstanden werden.[149] Die speichernde Stelle wurde in erster Linie technisch definiert. Einen technischen Ansatz konnte man auch dem, in Vorbereitung zum BDSG 1977 erstellten, sogenannten Steinmüller-Gutachten entnehmen. Dort war die Rede von dem Inhaber eines Informationssystems.[150] Neben der Definition der speichernden Stelle wurde die Verantwortungssphäre der speichernden Stelle durch die Negativdefinition des Dritten in § 2 Abs. 3 Nr. 2 BDSG 1977 eingegrenzt.

Zudem tauchte der sogenannte „Verbotsgrundsatz" das erste Mal in § 3 BDSG 1977 als „Zulässigkeit der Datenverarbeitung" auf. Das Phasenverständnis der Verarbeitung, auf das der „Verbotsgrundsatz" Bezug nimmt, findet sich in § 1 Abs. 1 BDSG 1977. Demnach ist es Aufgabe des Datenschutzes:

> *„[...] durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken."*

Auch wenn die verschiedenen Handlungen in Bezug auf die personenbezogenen Daten offensichtlich alle als „Datenverarbeitung"[151] aufgefasst wurden, war die Isolierung dieser schutzrelevanten Phasen[152] ein deutlich anderer Ansatz als der einheitliche Begriff der Verarbeitung unter der späteren DSRL. Dies gilt insbesondere im Hinblick auf die Entwicklungsoffenheit der Norm.[153] Eine weitere Besonderheit des BDSG 1977 war die Einschränkung des Anwendungsbereichs nach § 1 Abs. 2 S. 2 BDSG 1977 auf personenbezogene Daten, die zur Weiterübermittlung bestimmt waren.[154] Für Daten, die nicht weiter übermittelt werden sollten, galt nur § 6 BDSG 1977. Demnach waren technische und organisatorische Maßnahmen zu treffen, um die Ausführung der Vorschriften des BDSG 1977 zu gewährleisten.

Insgesamt zeigten sich im BDSG 1977 erste Schritte zur Definition eines allgemeinen Adressaten. Allerdings scheiterte dieser Versuch einer Festlegung noch

---

[149] *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 4 f.

[150] BT-Drs. VI/3826, S. 148, 154.

[151] BT-Drs. 7/5277, S. 6.

[152] Vgl. BT-Drs. 7/1027, S. 16, 20.

[153] Deutlich wird dies etwa durch Normen, die die verschiedenen Phasen der Datenverarbeitung isoliert regelten, so etwa §§ 9 ff., 23 ff. BDSG 1977.

[154] BT-Drs. 7/1027, S. 18, 39. Zwar hatten der Bundesrat die Streichung verlangt: BT-Drs. 7/1027, S. 33. Der Innenausschuss des BT hatte sich aber wiederum für die Beibehaltung entschieden: BT-Drs. 7/5277, S. 5.

häufig an der Erfassung unterschiedlicher Arten von speichernden Stellen, also etwa von öffentlich sowie nicht-öffentlichen Stellen, die wiederum nach geschäftsmäßiger oder nicht geschäftsmäßiger Verarbeitung unterschieden wurden.

Die nächste Reform des BDSG wurde erst im Jahr 1990 verabschiedet,[155] also knapp sieben Jahre nach dem Volkszählungsurteil des BVerfG.[156] Hinsichtlich des Adressaten zeigten sich keine gravierenden Änderungen. In der Definition der „speichernden Stelle" entfiel nur in § 3 Abs. 8 BDSG 1990 der Verweis auf den persönlichen Anwendungsbereich nach § 1 Abs. 2 BDSG 1977, wie ihn § 2 Abs. 3 Nr. 1 BDSG 1977 noch vorgesehen hatte. Dieser persönliche Anwendungsbereich fand sich dennoch in ähnlicher Form in § 1 Abs. 2 BDSG 1990. Die Unterscheidung zwischen der Verarbeitung nicht-öffentlicher Stellen für eigene bzw. geschäftsmäßig für fremde Zwecke entfiel. Nicht-öffentliche Stellen unterfielen gem. § 1 Abs. 3 Nr. 3 BDSG 1990 dem Anwendungsbereich, sofern sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiteten oder nutzten. Indirekt war hier bereits die später in der DSRL enthaltene Haushaltsausnahme vorgegriffen. Anstatt allerdings eine Ausnahme von der Anwendbarkeit festzulegen, war hier der Anwendungsbereich erst gar nicht eröffnet. Die Begriffe öffentliche und nicht-öffentliche Stellen selbst wurden in § 2 BDSG 1990 definiert. Dass zu diesem Zeitpunkt noch keine Anpassung des Begriffs der speichernden Stelle vorgenommen wurde, irritiert dahingehend, dass aufgrund des technologischen Fortschritts die Zuordnung der Verantwortlichkeit bereits zum damaligen Zeitpunkt durchaus hätte Probleme aufwerfen können.[157]

III. OECD-Guidelines (1980)

Die OECD-Guidelines[158] aus dem Jahr 1980,[159] als frühes supranationales Modell für datenschutzrechtliche Gesetze, definierten den Verantwortlichen im Annex zu den OECD Council Recommendations wie folgt:

> *„[Rn.] 1. For the purposes of these Guidelines:*

[155] Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes v. 20.12.1990, BGBl. I Nr. 73, S. 2954. Im Überblick: *Dammann*, NVwZ 1991, 640. Kritisch: *Walz*, CR 1991, 364.

[156] Kritisch hierzu: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 42. Zur Vorgeschichte: ebd., Rn. 52 ff.

[157] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 87 m.w.N.

[158] Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data (v. 23.09.1980).

[159] Zur Vorgeschichte: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 184.

a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;"

In dieser Definition waren bereits organisatorische und hierarchische Ansätze erkennbar („competent to decide", „regardless [...] by that party or by an agent on its behalf;").[160] Allerdings wurde die Festlegung des Verantwortlichen, bedingt durch das Wesen der OECD als internationaler Organisation, dem einzelstaatlichen Recht zugewiesen. Die OECD-Guidelines wiesen darüber hinaus einen eindeutigen Bezug zur Datei auf („contents of personal data"). Mit „use" und „content" waren bereits ähnliche Konzepte wie Zweck[161] und Mittel zugrunde gelegt, auch wenn diese sich noch auf die Datei bezogen.

Ausgeschlossen von der Einordnung als Verantwortliche sollten nach Rn. 40 des Explanatory Memorandum der Guidelines folgende Gruppen sein:

- *„a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes;*
- *b) data processing service bureaux which carry out data processing on behalf of others;*
- *c) telecommunications authorities and similar bodies which act as mere conduits; and*
- *d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities."*

Mit a) durften, ähnlich der Notifizierungspflicht in Art. 18 DSRL[162], den Aufsichtsbehörden vergleichbare Stellen gemeint worden sein. Die in b) genannten Gruppen wiederum erinnerten an den Auftragsverarbeiter nach Art. 17 Abs. 2 DSRL

[160] Siehe hierzu a. das Explanatory Memorandum der Guidelines in Rn. 40, abrufbar unter: *OECD*, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (abgerufen am 17.07.2024).

[161] Vgl. hierzu insb. die Zweckbindungsprinzipien in Rn. 9 und 10 der Guidelines.

[162] Eine vergleichbare Pflicht existiert in der DSGVO nicht mehr.

bzw. Art. 28 DSGVO. Die Telekommunikationsdienstleister in c) waren selbsterklärend und in der Richtlinie 2002/58/EG[163] („ePrivacy-RL“) ähnlich behandelt.[164] Die letzte Gruppe in d) schließlich durften dem Verantwortlichen untergeordnete bzw. weisungsgebundene Stellen und Personen sein. Eine ähnliche Regelung fand sich in Art. 16 DSRL bzw. Art. 29 DSGVO. Insgesamt hatten die OECD-Guidelines allerdings kaum Einfluss auf die DSRL.[165]

Die Definition des „data controllers“ wurde in den überarbeiten Guidelines[166] der OECD aus dem Jahr 2013 nicht verändert.[167] Allerdings wurde im dazu erarbeiteten Report[168] angeregt, Akteure jenseits des „data controllers“ in die Regulierung einzubeziehen sowie die Definition langfristig zu überarbeiten:

- *„The proposed revisions to the guidelines call upon member countries to "consider the role of actors other than data controllers, in a manner appropriate to their individual role". This provision intends to make policymakers aware that there are other actors who, while not covered by the concept of data controller, nevertheless influence the level of protection of personal data. While this provision provides one basis for addressing the evolving role of the individual, additional analysis is necessary to determine which measures (beyond awareness raising) may be appropriate.“*[169]
- *„The role of other actors (e.g. system designers): should the role of actors other than data controllers be better reflected in privacy frameworks? If so, to what extent?“*[170]
- *„The definition of data controller: should this definition be updated, in light of increased diversification and cross-organisational collaboration in data usage?“*[171]

[163] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

[164] Vgl. a. ErwGr 47 DSRL.

[165] *Brühann/Zerdick*, CR 1996, 429, 429.

[166] *OECD*, The OECD Privacy Framework, 2013.

[167] Die Pflichten wurden aber vertieft: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 186. Zu den überarbeiteten Guidelines a. Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 147.

[168] *OECD*, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines.

[169] *OECD*, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, 9.

[170] *OECD*, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, 11.

[171] *OECD*, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, 11.

IV. Übereinkommen Nr. 108 des Europarates (1981)

Das Übereinkommen Nr. 108 des Europarates[172] aus dem Jahr 1981 ist neben der DSRL und der DSGVO zweifelsohne der bekannteste nicht rein nationale Normtext im Bereich des Datenschutzrechts. Die ursprüngliche Version[173] des Übereinkommens aus dem Jahr 1981 findet regelmäßig Erwähnung, wenn es um Inspirationen für die DSRL geht.[174] Das Übereinkommen selbst entstand wiederum im Meinungsaustausch mit der OECD.[175] *Simitis* beschreibt es als Zusammenfassung der Grundsätze, die die internationale Datenschutzdiskussion beherrschten.[176] In dem Übereinkommen Nr. 108 wird der Verantwortliche wie folgt definiert:

> *„Art. 2 lit. d*
> *"controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.“*

Dazu ergänzt der Explanatory Report:

> *„By "controller of the file" the convention means only the person or body ultimately responsible for the file, not persons who carry out the operations according to the instructions given by the controller of the file.“*[177]

Ähnlich wie die OECD-Guidelines überließ die Definition des Übereinkommens Nr. 108 des Europarates die Festlegung, wer Verantwortlicher ist, entsprechend dem Wesen des Europarates als internationaler Organisation, dem einzelstaatlichen Recht.[178] Anstatt „party“, wie in der OECD-Definition, fand sich in dieser Definition

---

[172] Council of Europe, Nr. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[173] Das Übereinkommen wurde am 18.05.2018 mit einem ergänzenden Protokoll (CETS No. 223) abgeändert.

[174] Vgl. allein ErwGr 11 DSRL.

[175] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 137, 184 ff.

[176] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 137, 154 ff.

[177] *Council of Europe*, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981, Rn. 32.

[178] Vgl. a. *Council of Europe*, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981, Rn. 32; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10.

eine nicht abschließende Aufzählung potenzieller Subjekte, die einen Verantwortlichen darstellen konnten. Zwar musste, ähnlich wie in der OECD-Definition, der Verantwortliche über den Inhalt der Datei entscheiden, daneben sollte der Verantwortliche aber statt über die Nutzung über den Zweck der Datei entscheiden. Anders als die OECD-Definition maß die Definition des Europarates auch der Entscheidung über die Verfahren mit denen Daten verarbeitet werden sollten Bedeutung bei. Darin deutete sich bereits das Definitionselement „Mittel", wie es die DSRL später verwendete, an. Abweichend von der OECD-Definition ließ die Definition des Europarates jedoch nicht die organisatorische Zurechnung anderer Subjekte, etwa durch eine Auftragsverarbeitung, erkennen.[179] Dass Art. 2 lit. d des Übereinkommens Nr. 108 nicht nur den technischen Verantwortlichen erfassen sollte, wurde aber durch den Explanatory Report klargestellt.[180] Ein weiterer wichtiger Unterschied zwischen den OECD-Guidelines und dem Übereinkommen Nr. 108 des Europarates war zudem, dass sich die Definition des Europarates nur auf „automated personal data" erstreckt, also nach den Definitionen in Art. 2 lit. b und c des Übereinkommens Nr. 108 nur auf personenbezogene Daten, die komplett oder teilweise automatisch verarbeitet wurden.[181]

V. DSRL (1995)

Die DSRL nahm in weiten Teilen Bezug auf das Übereinkommen Nr. 108 des Europarates.[182] Dies galt auch für die Definitionen und insbesondere für den (für die Verarbeitung) Verantwortlichen.[183] Das allgemeine Verhältnis zwischen Übereinkommen Nr. 108 des Europarates und der DSRL konnte man als kompatibel

[179] Vgl. das Definitionselement: „by that party or by an agent on its behalf" der OECD-Definition.

[180] *Council of Europe*, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981, Rn. 32.

[181] Dies wurde am 15.06.1999 dahingehend ergänzt, dass nach Art. 2 lit. c des Übereinkommen Nr. 108 des Europarates durch Deklaration seitens des Vertragsstaats auch nicht-automatisch verarbeitete Dateien einbezogen werden konnten.

[182] Siehe allein ErwGr 11 DSRL; Ehmann/Helfrich DSRL, Art. 2, Rn. 1; Grabitz/Hilf[40]/*Brühann*, A 30 Vorbem. DSRL, Rn. 60. Daneben nahm die DSRL a. Ansätze aus den mitgliedstaatlichen Datenschutzgesetzen auf: *Monreal*, CR 2019, 797, Rn. 15; *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 15. Im Hinblick auf den (für die Verarbeitung) Verantwortlichen sind Anleihen aus den Mitgliedstaaten allerdings nicht ersichtlich.

[183] BT-Drs. 12/8329, S. 12 ff.; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 4; Ehmann/Helfrich DSRL, Art. 2, Rn. 2.

und komplementär beschreiben.[184] Aufgrund des Rückgriffs auf mitgliedstaatliche Elemente, die wiederum im wirtschaftlichen und technischen Kontext der siebziger und frühen achtziger Jahre entstanden, wurde die DSRL aber auch als „in wesentlichen Elementen strukturkonservativ" bezeichnet.[185]

Im ursprünglichen Entwurf[186] der Kommission zur DSRL aus dem Jahr 1990 war der Verantwortliche wie folgt definiert:

> *„Art. 2 lit. e*
> *„Verantwortlicher der Datei": die natürliche oder juristische Person, Behörde, Dienststelle oder jede andere Einrichtung, die nach dem Gemeinschaftsrecht oder den einzelstaatlichen Rechtsvorschriften eines Mitgliedstaats zuständig ist, darüber zu entscheiden, welche Zweckbestimmung die Datei verfolgt, welche Arten personenbezogener Daten gespeichert und mit welchen Vorgängen sie verarbeitet werden sollen sowie welche Dritte Zugang zu den Dateien haben dürfen."*[187]

Nach der Begründung der Kommission[188] passte der Entwurf die Definition des Übereinkommens Nr. 108 des Europarates um einen Verweis auf das Gemeinschaftsrecht[189] an und definierte den Verantwortlichen zusätzlich danach, wer bei direkten (Datei-)Abfragen den Zugang genehmigte. Ähnlich wie in der Definition des Übereinkommens Nr. 108 war Verantwortlicher nur derjenige, dem das Gemeinschaftsrecht oder das mitgliedstaatliche Recht diese Rolle zuwies. Verantwortlicher war also nicht derjenige, der faktisch über die Datei entschied, sondern derjenige, der dies rechtlich durfte.[190]

Im geänderten Entwurf der Kommission[191] aus dem Jahr 1992 lautete die Definition wie folgt:

---

[184] ErwGr 11 DSRL; Grabitz/Hilf/*Brühann*, A 30 Vorbem. DSRL, Rn. 61 ff.

[185] *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 458.

[186] Vorschlag v. 18.07.1990, veröffentlicht in BR-Drs. 690/90.

[187] BR-Drs. 690/90, S. 52 f.

[188] BR-Drs. 690/90, S. 19.

[189] Mit der Gemeinschaft ist hier die Europäische Gemeinschaft (EG) als Vorläufer der Europäischen Union (EU) gemeint.

[190] *Monreal*, ZD 2014, 611, 611. Die Möglichkeit der gesetzlichen Festlegung eines Verantwortlichen bestand in der finalen Version in Art. 2 lit. d S. 2 DSRL aber wieder, vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10.

[191] Vorschlag v. 15.10.1992, veröffentlicht in BT-Drs. 12/8329.

> *„Art. 2 lit. d*
> *„Verantwortlicher der Verarbeitung": die natürliche oder juristische Person, Behörde, Dienststelle oder jede andere Einrichtung, die personenbezogene Daten verarbeitet oder verarbeiten läßt und über Zweck und Ziel der Verarbeitung, die verarbeiteten personenbezogenen Daten und die Verarbeitungsverfahren, die auf sie angewandt werden, sowie darüber entscheidet, welche Dritte Kenntnis von den genannten Daten haben dürfen;"*[192]

Die Definition im geänderten Entwurf enthielt eine wesentliche Neuerung gegenüber der Definition des Übereinkommens Nr. 108, nämlich die Abkehr vom Bezugsobjekt der Datei,[193] hin zum Bezugsobjekt der Verarbeitung.[194] Daneben stellte diese Definition deutlich heraus, dass der Verantwortliche derjenige war, der organisations- oder hierarchiebedingt über die Verarbeitung entscheiden konnte[195] und nicht mehr derjenige, dem dies rechtlich zugewiesen war.[196] Ob auch rechtmäßig über die Verarbeitung entschieden wurde, war unerheblich.[197] Ähnlich wie beim Begriff der Verarbeitung in der DSRL, der nicht dem Phasenmodell des BDSG 1990 entsprach,[198] sondern abstrakter und flexibler gestaltet war,[199] zeigt sich dieser höhere Abstraktionsgrad auch bei der Bestimmung des (für die Verarbeitung) Verantwortlichen.[200] Die Art. 29-Datenschutzgruppe sah für diese Änderung vor allem zwei Gründe. Zum einen läge nicht immer eine formelle Zuweisung der

---

[192] BT-Drs. 12/8329, S. 67.

[193] Siehe hierzu: Dammann/Simitis DSRL/*Simitis*, Einleitung, Rn. 21; Ehmann/Helfrich DSRL, Art. 1, Rn. 7 ff. Das HDSG hatte sich schon 1986 vom Bezugsobjekt der Datei, zugunsten der Verarbeitung, verabschiedet.

[194] BT-Drs. 12/8329, S. 6, 13; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 3; Ehmann/Helfrich DSRL, Art. 2, Rn. 39 ff. Der Begriff der Verarbeitung wiederum wird nach der Begründung der Kommission zum geänderten Vorschlag weit verstanden: BT-Drs. 12/8329, S. 13.

[195] BT-Drs. 12/8329, S. 13 f.; Ehmann/Helfrich DSRL, Art. 2, Rn. 44.

[196] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10 f.; Eingehender: *Monreal*, CR 2019, 797, Rn. 16; *Alsenoy*, CLSR[28] (2012), 25, 28.

[197] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11 f.

[198] Dazu: Kapitel 1 B. II. BDSG (1977).

[199] Insofern ist a. eine Überarbeitung des Fachrechts spätestens mit der DSGVO überfällig geworden: *Eickelpasch*, RdV 2017, 219, 220.

[200] Vgl. für den Verantwortlichen: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 63.

Verantwortlichkeit, etwa per Gesetz, Vertrag oder aufgrund der damaligen Meldepflicht (gem. Art. 18 DSRL) vor. Zum anderen müsse eine formelle Zuweisung nicht notwendigerweise den faktischen Gegebenheiten entsprechen.[201]

In der endgültigen Version der DSRL schließlich wurde der (für die Verarbeitung) Verantwortliche wie folgt definiert:

> *„Art 2. lit. d*
> *„für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;"*

Eine wesentliche Neuerung der endgültigen Version der DSRL war, dass das Konzept der gemeinsam Verantwortlichen hier zum allerersten Mal auftauchte.[202] Diese Änderung ging zurück auf die Position des EU-Parlament zur DSRL.[203] Die Kommission führte in ihrer Stellungnahme zur Position des EU-Parlaments aus, dass jeder der gemeinsam Verantwortlichen sich an die Verpflichtungen der DSRL zu halten habe.[204] Die weiteren Änderungen innerhalb der Definition gegenüber dem geänderten Entwurf der Kommission lassen sich nicht nachvollziehen. Sie stellen wohl vor allem eine Raffung der Definition durch den Rat dar.[205]

Weitere Ausführungen zur Bestimmung des (für die Verarbeitung) Verantwortlichen enthielt die DSRL nicht. Allein ErwGr 47 DSRL[206] führte aus, dass ein Anbieter von Telekommunikationsdiensten (in der Regel) nicht für die Inhalte der

---

[201] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[202] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5, 22.

[203] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[204] KOM (95) 375 endg. - COD 287, S. 3.

[205] Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 19; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 15 ff.

[206] Eingehend hierzu: Ehmann/Helfrich DSRL, Art. 2, Rn. 45 ff.

Kommunikation, die er übermittelt, verantwortlich sein sollte.[207] Für die Daten, die im Rahmen des Betriebs des Dienstes anfallen, sollte er hingegen (in der Regel) verantwortlich sein.

Der die DSRL ergänzende Rahmenbeschluss des Rates[208] für Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aus dem Jahr 2008 definierte den für die Verarbeitung Verantwortlichen nahezu identisch wie die DSRL als:

> *„Art. 2 lit. i*
> *„für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;"*

In der Definition des Rahmenbeschlusses fiel nur die Festlegung des Verantwortlichen durch mitgliedstaatliches oder Unionsrecht weg.[209]

VI. BDSG (2001)

1. Überblick

In Deutschland gab es, wie dargestellt, bereits vor Verabschiedung der DSRL ein Datenschutzgesetz im Rahmen des BDSG 1990. Daher kam es bei der Umsetzung der DSRL[210] in das deutsche Recht zu gewissen Friktionen.[211] So definierte § 3 Abs. 7 BDSG 2001, nach Umsetzung der DSRL im Jahr 2001,[212] die verantwortliche Stelle als:

> *„[...] jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt,*

[207] Sondern der Absender der Kommunikation.

[208] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Dieser Rahmenbeschluss wurde durch die DSRL-JI abgelöst.

[209] Dies war im ursprünglichen Kommissionsentwurf noch vorgesehen: KOM (2005) 475 endg. Warum darauf verzichtet wurde, lässt sich nicht erschließen.

[210] Dazu: *Abel*, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 51 ff.

[211] Mahnend bereits im Vorfeld: *Brühann/Zerdick*, CR 1996, 429, 430. Siehe a. Kühling/Buchner/*Hartung*, Art. 28 DS-GVO, Rn. 25; Simitis/Hornung/Spiecker/*Petri*, Art. 28 DSGVO, Rn. 8.

[212] Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze v. 18.05.2001, BGBl. I Nr. 23, S. 904.

verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt."

Damit legte das BDSG 2001 den Fokus auf die Verarbeitung als das maßgebliche Definitionselement für die verantwortliche Stelle. Trotz vermeintlicher Umsetzung der DSRL fand dessen Definitionselement der Entscheidung (über die Zwecke und Mittel der Verarbeitung), jedenfalls im Wortlaut von § 3 Abs. 7 BDSG 2001, keine Berücksichtigung.[213] Stattdessen wurde der Begriff der „speichernden Stelle" durch die „verantwortliche Stelle" ersetzt.[214] Maßgeblich für das Verständnis der Stelle waren § 1 Abs. 2 und § 2 BDSG 2001.[215] Dort wurden öffentliche und nicht-öffentliche Stellen definiert. Ebenso wie das Definitionselement der Entscheidung suchte man auch die gemeinsam Verantwortlichen in § 3 Abs. 7 BDSG 2001 vergeblich.[216] Diese mussten erst durch die unionsrechtskonforme Auslegung der Norm in diese hineingelesen werden.[217]

Insgesamt zeigte sich im BDSG, jedenfalls vor Umsetzung der DSRL,[218] eine gewisse Varianz der Begriffe hinsichtlich der Normadressaten. Neben dem Vorgängerbegriff des BDSG 1990 – der „speichernden Stelle" – fand sich häufig etwa auch der Begriff der „übermittelnden Stelle". Solche Begriffe wurden nicht eigens definiert. Folglich ließ sich der Bedeutungsgehalt dieser Begriffe maximal aus der Definition der entsprechenden Verarbeitungsschritte ableiten.[219] Auch heute noch findet sich in Normen wie § 6 Abs. 2 S. 5 BVerfSchG der Begriff der „speichernden Stelle". Dabei soll für das Verständnis dieses Begriffs auf die allgemeinen Vorschriften des Datenschutzrechts zurückgegriffen werden. Ein solcher Rückgriff auf die „allgemeinen Vorschriften des Datenschutzrechts" und somit die Definitionen des BDSG a.F. ist aber seit Inkrafttreten der DSGVO nicht mehr möglich.[220]

---

[213] Vgl. a. *Lewinski/Herrmann*, ZD 2016, 467, 469; Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 3; G/S/S/V/*Kramer*, Art. 4 Nr. 7 DSGVO, Rn. 6. Kritisch: *Brühann*, DuD[28] (2004), 201, 205 Fn. 33.

[214] BT-Drs. 14/4329, S. 33; BeckOK DatenschutzR[28]/*Schild*, § 3 BDSG a.F., Rn. 108.

[215] *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 9, 12, 14.

[216] Die verantwortliche Stelle wurde also grds. als singuläre Stelle verstanden, siehe a. Simitis/*Dammann*, § 3 BDSG a.F., Rn. 226.

[217] *Monreal*, ZD 2014, 611, 614 m.w.N.; BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 23. *Kremer*, CR 2019, 225, Rn. 1 geht hingegen von einer Unionsrechtswidrigkeit aus.

[218] Vgl. Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 13.

[219] Eventuell könnte man hierin a. einen Gebrauch der Spezifizierung des Verantwortlichen nach Art. 2 lit. d S. 2 DSRL erkennen. Da die Uneinheitlichkeit der Begriffe allerdings bereits seit dem BDSG 1977 (vgl. etwa § 10) bestand, ist dies eher unwahrscheinlich.

[220] Der Begriff der „speichernden Stelle" existiert seit der Umsetzung der DSRL im BDSG 2001 nicht mehr. Auch die Definitionen der einzelnen Verarbeitungsschritte finden sich seit Umsetzung der DSGVO

Wesentliche Änderungen an der verantwortlichen Stelle, dem Auftragsverarbeiter oder dem Dritten wurden bei den Änderungen des BDSG 2001 im Jahr 2003 und 2009 nicht vorgenommen.[221] Insgesamt kann man die Umsetzung der DSRL als lückenhaft erachten.[222]

2. Technischer Ansatz

Im Vergleich zur DSRL ist besonders auffallend, dass das BDSG 2001 die verantwortliche Stelle anhand der Verarbeitung[223] als solcher bestimmte.[224] Eine verantwortliche Stelle war also, wer entweder selbst personenbezogene Daten verarbeitete oder dies durch andere im Auftrag vornehmen ließ. So ließ sich die verantwortliche Stelle auch vom Auftragsverarbeiter aus rückbestimmen, da der Anknüpfungspunkt die Verarbeitung im Sinne des technischen Prozesses war. Die DSRL knüpfte zwar grundsätzlich auch an die Verarbeitung als Bezugspunkt für die Verantwortlichkeit an. Anstatt allerdings die Verarbeitung technisch[225] anhand der Durchführung oder rechtlich per Norm[226] einer bestimmten Stelle zuzuschreiben, orientierte sich die DSRL an der Entscheidung über die Zwecke und Mittel der Verarbeitung. Damit war die Definition der DSRL anpassungsfähiger an komplexe Sachverhalte.[227]

Inwiefern sind diese unterschiedlichen Anknüpfungspunkte relevant? Grundsätzlich wird mit einer technischen oder einer organisatorischen „Herrschaft“[228] über die Verarbeitung notwendigerweise auch eine Entscheidungsmacht einhergehen. Allerdings impliziert der Fokus auf die Durchführung und somit den technischen Prozess der Verarbeitung auch eine Verfügungsgewalt über die Daten.[229] Dagegen setzt

---

nicht mehr in § 2 BDSG.

[221] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 102.

[222] Deutlich schärfer: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 99 ff.

[223] Genauer der Erhebung, Verarbeitung und Nutzung. Dabei wurde die Verarbeitung in § 3 Abs. 4 BDSG 2001 wiederum in verschiedene Phasen unterteilt.

[224] Simitis/*Dammann*, § 3 BDSG a.F., Rn. 224; Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 9, 20; kritisch: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 63.

[225] Wie das BDSG 1990.

[226] Wie das Übereinkommen Nr. 108 des Europarates.

[227] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 63.

[228] Vgl. etwa Taeger/Gabel/*Buchner*, § 3 BDSG a.F., Rn. 53. Vgl. zur Verfügungsgewalt: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 102, 107.

[229] Vgl. etwa *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 150 f. Vgl. zur Kontrolle der Verarbeitung anstatt der Daten a. *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 28 f. Eingeschränkt, v.a. im Hinblick auf die Auftragsverarbeitung: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 225, 227.

das Kriterium der Entscheidung über die Verarbeitung vielmehr an einer strukturellen und funktionalen Beeinflussung an.[230] Zweifelsohne gibt es zwischen beiden Ansätzen erhebliche Schnittmengen. Allerdings wird bei einer Entscheidung über die Zwecke und Mittel der Verarbeitung i.S.d. DSRL die Orientierung an den tatsächlichen Umständen der Verarbeitung klarer. Der Vorteil, die Verantwortlichkeit anhand tatsächlicher Umstände zu bestimmen, liegt gegenüber der formalistischen Beurteilung aufgrund von technischer Beherrschbarkeit oder organisatorischer Zugehörigkeit darin, Umgehungskonstruktionen entgegen einer Verantwortlichkeit vorzubeugen.[231] Festhalten lässt sich anhand dieser vermeintlich einheitlichen, aber dennoch im Detail unterschiedlichen Definitionen, dass das BDSG 2001 nach Umsetzung der DSRL immer noch einer stark technischen Sichtweise entsprach.[232] Inwiefern in Bezug auf die verantwortliche Stelle von einer inhaltlich korrekten Umsetzung gesprochen werden konnte, ist daher zweifelhaft.[233]

3. Auftragsverarbeitung

Im Gegensatz zur DSRL fand sich der Auftragsverarbeiter nicht in der allgemeinen Definitionsnorm des BDSG 2001 in § 3. Die Definition ergab sich vielmehr indirekt aus § 11 Abs. 1 S. 1 und Abs. 3 S. 1 BDSG 2001. So wurde einerseits die Verantwortlichkeit der verantwortlichen Stelle für die Verarbeitung durch den Auftragsverarbeiter festgelegt. Andererseits durfte „der Auftragnehmer [...] die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen." Dabei war strittig, ob die Weisungsgebundenheit Voraussetzung oder Konsequenz der Auftragsverarbeitung war. Die Definition der DSRL setzte sie nicht explizit voraus. Im Zusammenhang mit Art. 16 und 17 Abs. 3 1. Spiegelstrich DSRL lag es jedoch nahe, sie als Pflicht aus dem Auftragsverarbeitungsverhältnis zu verstehen.

4. Dritter

Auch die Definition des Dritten in § 3 Abs. 8 S. 2, 3 BDSG 2001 wirkte uneindeutig.[234] So war ein Dritter nach S. 2 zunächst jede Person oder Stelle außerhalb der

[230] Vgl. Dammann/Simitis (Hrsg.), EG-Datenschutzrichtlinie, 1997, Rn. 13; Ehmann/Helfrich DSRL, Art. 2, Rn. 43 f. Verwunderlich ist dabei die unterschiedliche Kommentierung durch dieselbe Person.

[231] So i.E. a.: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 63.

[232] *Monreal*, ZD 2014, 611, 614; mit ähnlicher Kritik schon 2001: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 63.

[233] So *Monreal*, PinG 2017, 216, 220.

[234] So ist „Dritter [...] jede Person oder Stelle außerhalb der verantwortlichen Stelle." Dies wird im

verantwortlichen Stelle. S. 3 legte dann aber sogleich Ausnahmen von S. 2 für den Betroffenen und Auftragsverarbeiter fest. Dies war für das Verständnis der ohnehin schwer nachvollziehbaren Negativdefinition nicht förderlich. Keine Erwähnung fanden auch die der verantwortlichen Stelle oder dem Auftragsverarbeiter unterstellten Personen, die unter deren jeweiliger Verantwortung befugt waren, Daten zu verarbeiten. Aufgrund des Datengeheimnisses in § 5 BDSG 2001 war allerdings eine organisatorische Privilegierung dieser Personen anzunehmen. Potenziell unionswidrig war zudem die Einschränkung der Privilegierung der Auftragsverarbeitung auf das Gebiet der EU und des EWR.[235] Denn die umzusetzende DSRL schränkte den Anwendungsbereich der Auftragsverarbeitung gerade nicht auf Auftragsverarbeiter im Unions- bzw. EWR-Gebiet ein.

5. Normadressat TMG

Hinsichtlich des TMG[236] war zudem lange Zeit strittig, ob der Diensteanbieter aus § 2 Abs. 1 TMG[237] isoliert Normadressat der datenschutzrechtlichen Normen des TMG (§§ 11 - 15a TMG a.F.) sein konnte oder ob ein Rückgriff auf die verantwortliche Stelle aus § 3 Abs. 7 BDSG a.F. via § 12 Abs. 3 TMG a.F. notwendig war und damit eine doppelte Qualifizierung des Normadressaten.[238] Alternativ konnte man auch ohne Rückgriff auf die Verweisungsnorm anhand der Verarbeitung eine normspezifische doppelte Qualifikation als verantwortliche Stelle im Sinne von § 3 Abs. 7 BDSG a.F. herleiten. Da das TMG als solches allerdings nicht die ePrivacy-RL umsetzt[239] und somit nicht von Art. 95 DSGVO gedeckt ist, dürfte sich dieser Streit seit Geltungsbeginn der DSGVO erledigt haben. Ähnliche Unklarheiten bestehen im Rahmen des TDDDG, in das die datenschutzrechtlichen Normen des TMG aufgegangen sind, nicht.

---

nächsten Satz ergänzt um „Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen."

[235] Vgl. *Monreal*, ZD 2014, 611, 615 f.

[236] Vorgängergesetz des DDG sowie TDDDG.

[237] Nun § 1Abs. 4 Nr. 5 DDG.

[238] So etwa: OVG Schleswig, Urteil vom 04.09.2014 – 4 LB 20/13 = ZD 2014, 643, 644; *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 149. Anders: BeckRTD-Komm/*Bizer/Hornung*, § 12 TMG, Rn. 39.

[239] *Nebel/Richter*, ZD 2012, 407, 408.

VII. Modernisiertes Übereinkommen Nr. 108 des Europarates (2018)

Das Übereinkommen Nr. 108 des Europarates aus dem Jahr 1981 wurde am 18.05.2018 mit einem ergänzenden Protokoll[240] abgeändert.[241] Dadurch wurde auch die Definition des Verantwortlichen abgeändert, sie lautet nun:

> *„Art. 2 lit. d*
> *"controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;"*

Die Definition des Verantwortlichen bezieht sich nun auf die Verarbeitung, weggefallen ist hingegen der Bezug auf die Datei. Die Verarbeitung wird wiederum in Art. 2 lit. b, sehr ähnlich zur DSGVO, weit definiert. Es muss sich hierbei nicht mehr um eine automatische Verarbeitung handeln.[242] Zudem ist die Festlegung der Verantwortlichkeit durch das einzelstaatliche Recht entfallen.[243] Auffällig ist, dass sich die Entscheidungsmacht anhand des Wortlauts nicht auf spezifische Aspekte wie Zwecke, Datenkategorien oder Verfahren der Verarbeitung bezieht, sondern ganz allgemein auf die Verarbeitung. Der Explanatory Report bezieht die Entscheidung dennoch auf die Zwecke und Mittel der Verarbeitung.[244] Die Zwecke seien die Gründe, die die Verarbeitung rechtfertigen und sollten daher bei der Feststellung der Verantwortlichkeit besonders beachtet werden. Daneben sollten aber weiterhin die Kontrolle über Verarbeitungsverfahren, über die verwendeten Daten und über den Zugang zu den Daten berücksichtigt werden. Neu ist schließlich die Erwähnung von gemeinsam Verantwortlichen. Diese könnten für verschiedene Aspekte der Verarbeitung verantwortlich sein, ohne dass dies ihre Qualifizierung als gemeinsam Verantwortliche verhindere.[245]

---

[240] CETS No. 223.

[241] Zum Reformprozess: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 177. Zur Neufassung: BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 87a.

[242] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 21.

[243] Nach dem Explanatory Report kann sich die Verantwortlichkeit nichtsdestotrotz aus rechtlicher Zuweisung oder anhand des Sachverhalts ergeben: *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 22.

[244] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 22. Vgl. a. Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 146 f.

[245] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection

Aufgrund des Bezuges auf die Entscheidungsmacht ist nicht mehr notwendigerweise derjenige Akteur Verantwortlicher, der die finale Entscheidung über die Verarbeitung trifft. Vielmehr sind alle Akteure mit tatsächlicher Entscheidungsmacht für die maßgebliche Verarbeitung gemeinsam Verantwortliche. Insgesamt handelt es sich, im Vergleich zur DSGVO, um eine sehr komprimierte Definition. Neben der Änderung der Definition des Verantwortlichen wurden zudem die Begriffe des „recipient" bzw. Empfängers und des „processor" bzw. Auftragsverarbeiters neu eingeführt. Die Definition des Auftragsverarbeiters ist fast identisch mit der DSGVO. Maßgeblich für die Feststellung, ob eine Stelle Verantwortlicher oder Auftragsverarbeiter ist, soll zum einen das Handeln im Auftrag, zum anderen aber vor allem die Weisungsgebundenheit[246] sein.[247] Die Weisungen stellen dabei die Grenzen dessen dar, was der Auftragsverarbeiter mit den Daten machen darf.[248]

VIII. Gesetzgebung der Europäischen Union im digitalen Bereich

Trotz der zuletzt zahlreichen Gesetzgebungsverfahren der Europäischen Union im Bereich des Datenrechts finden sich dort keine Modifikationen am Konzept des Verantwortlichen. Der Data Act[249] legt in ErwGr 7 sowie Art. 1 Abs. 5 fest, dass der Data Act („DA") unbeschadet der DSGVO gilt. Er ergänze die DSGVO und lasse sie unberührt. Gleiches gilt für den Data Governance Act[250] („DGA"), der in ErwGr 4 und Art. 1 Abs. 3 entsprechendes festlegt. Auch der Digital Markets Act[251] („DMA") trifft in ErwGr 12 solche Anordnungen. Ebenso legt der Digital Services Act („DSA") als

of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 22.

[246] Wobei ein Angestellter des Verantwortlichen nicht Auftragsverarbeiter sein kann: *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 24.

[247] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 22.

[248] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 24.

[249] Verordnung (EU) 2023/2854 des europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).

[250] Verordnung (EU) 2022/868 des europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt).

[251] 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).

Nachfolger der e-Commerce-RL[252] in ErwGr 10 und Art. 2 Abs. 4 lit. g fest, dass er die DSGVO unberührt lässt. Der Entwurf des AI Acts („AIA“) nach erster Lesung im Parlament schließlich lässt auch die DSGVO unberührt.[253]

IX. Kritik der fehlenden Evolution des Konzeptes

Wie dargestellt hat das Konzept des Verantwortlichen seit der verspäteten Verankerung im BDSG 1977 durch die „speichernde Stelle“ nur zwei gravierende Veränderungen durch die DSRL erfahren. Diese bestanden darin, die Verantwortlichkeit von der Entscheidung über die Zwecke und Mittel der Verarbeitung abhängig zu machen sowie die gemeinsame Verantwortlichkeit einzuführen. Abseits dessen wurden das Konzept des Verantwortlichen nicht weiter ausdifferenziert oder weiterentwickelt.[254] Auch die Auftragsverarbeitung war bereits in der frühen datenschutzrechtlichen Gesetzgebung erkennbar.[255]

Zur Zeit des Erlasses des BDSG 1977 und anderer nationaler Datenschutzgesetze fanden sich Computer meist in Universitäten, Regierungseinrichtungen oder in Großunternehmen.[256] Die Verarbeitung personenbezogener Daten im öffentlichen oder privaten Sektor erfolgte daher weitestgehend vorhersehbar und statisch.[257] Verglichen mit heute war die Rechenleistung begrenzt und es gab kaum eine Vernetzung der Systeme untereinander. Daher konzentrierte sich das damalige Datenschutzrecht auf die Regulierung eben solcher Verarbeitungskontexte, also individuell agierende Akteure und nicht vielfach vernetzte, gegenseitig voneinander abhängige Akteure. Auch in den frühen 80er Jahren, also zur Zeit der Verabschiedung des Übereinkommen Nr. 108 des Europarates, waren – trotz eines zunehmenden Trends zur Vernetzung – Großrechner aufgrund ihrer Rechenleistung immer noch das vorherrschende Mittel der Verarbeitung von Daten.[258] Zum Zeitpunkt der Verabschiedung der DSRL im Jahr 1995 bestand durch die zunehmende Vernetzung

[252] Richtlinie 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").

[253] ErwGr 10 und Art. 2 Abs. 7 AIA-E.

[254] Vgl. allgemein zum Datenschutzrecht: *Roßnagel*, MMR 2005, 71, 71. Speziell zur speichernden Stelle: *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 457 f.

[255] Vgl. § 2 Abs. 3 Nr. 2, § 8 BDSG 1977.

[256] *Alsenoy*, CLSR[28] (2012), 25, 27 m.w.N.

[257] Dabei war der Fokus, im Gegensatz zu heute, vor allem auf der staatlichen Datenverarbeitung: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 23 f.

[258] *Alsenoy*, CLSR[28] (2012), 25, 27 f. m.w.N.

von PCs und steigende Zahl von Internetzugängen bereits eine stark veränderte Situation. Durch das Internet und dessen globale Natur bedingte Entwicklungen wie zunehmende Dezentralisierung, geringere Hürden für Datenaustausch und die weltweite, öffentliche Verfügbarkeit waren bei Verabschiedung der DSRL im Jahr 1995 zwar bereits erkennbar. Sie konnten aber aufgrund des langwierigen Gesetzgebungsprozesses nicht mehr berücksichtigt werden.[259] Auch in der deutschen Literatur wurde 2000, also kurz vor Umsetzung der DSRL, noch kritisiert, dass das Regelungsmodell der „speichernden Stelle" noch von Einzelunternehmen ausginge, die entweder Daten selbst oder allenfalls durch Auftragsverarbeiter verarbeiten ließen.[260] An dieser Grundkonzeption der Verantwortlichkeit hat sich auch mit der DSGVO und dem modernisierten Übereinkommen Nr. 108 des Europarates nichts fundamental geändert.[261] Es gibt weiterhin keine Varianten oder Abstufungen der Verantwortlichkeit auf der Normebene.[262] Entweder eine Stelle ist verantwortlich oder sie ist es nicht.

Es ließe sich nun einwenden, dass durch den Auftragsverarbeiter gem. Art. 28 DSGVO und die gemeinsam Verantwortlichen gem. Art. 26 DSGVO weitere Beteiligungsszenarien berücksichtigt werden können. Allerdings sorgt das Konzept des Auftragsverarbeiters[263] eben gerade nicht für eine Ausdifferenzierung der Verantwortlichkeit. Im Gegenteil, es verhindert diese, indem die Verantwortlichkeit weitestgehend dem Auftraggeber zugewiesen wird.[264] Diese Zuweisung ist logische Folge des Erfordernisses der Weisungsgebundenheit.[265] Berücksichtigt wird damit nur das berechtigte Anliegen von Verantwortlichen Datenverarbeitungen zwecks Expertise, Know-How oder Technik an Andere auszulagern. Eine Abstufung der Verantwortung findet damit gerade nicht statt.[266] Gleiches gilt für die gemeinsam Verantwortlichen. Indem alle Verantwortlichen nach außen grundsätzlich für alle

[259] *Alsenoy*, CLSR[28] (2012), 25, 28.

[260] *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 457.

[261] Vgl. zur Entwicklung der Datenschutzgesetze insgesamt bis 2012: *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 88.

[262] Anders als etwa der Name Datenschutz-Grundverordnung vermuten lassen würde.

[263] Dazu: Kapitel 2 G. Der Auftragsverarbeiter als Abgrenzungsobjekt.

[264] Vgl. Art. 28 Abs. 3 lit. a DSGVO.

[265] Insofern fängt eine gemeinsame Verantwortlichkeit sinnvollerweise bereits bei einer nicht weisungsgebundenen quasi-Auftragsverarbeitung an. Denn in diesem Fall wird ja bereits über die Mittel entschieden, wenn a. auf sehr niedrigem Niveau.

[266] Vgl. a. *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 1: „Together, these concepts [controller and processor] provide the very basis upon which responsibility for compliance is allocated."

Pflichten, die sich aus der Verantwortlichkeit ergeben, gleichwertig verantwortlich bleiben, wird auch hier keine Ausdifferenzierung erreicht.[267] Es wird schlicht eine Mehrzahl von Beteiligten an einer Verarbeitung erfasst.[268]

Folglich bleibt es bei dem bereits im HDSG 1970 festgelegten Rollenmodell des Datenschutzrechts mit den drei bzw. vier Rollen, also dem Verantwortlichen, dem diesem zuzurechnenden Auftragsverarbeiter, der betroffenen Person und dem Dritten.[269] Die Einteilung in die positiven[270] Rollen des Verantwortlichen, des Auftragsverarbeiters und der betroffenen Person wird als „lineares Modell" bezeichnet.[271] Dieses Modell zeichnet sich durch zentralisierte Systeme von Datenverarbeitungen aus, bei denen jeweils von unabhängigen Beziehungen zwischen Verantwortlichen und betroffenen Personen ausgegangen wird. Es spiegelt im Kern die Verarbeitungsrealität zur Entstehungszeit der DSRL wider. In diesem Modell hat der Verantwortliche die finale Entscheidungskompetenz über die Datenverarbeitung und entscheidet frei über die Integration von fremden Systemen oder Diensten. Ob dieses Modell einer zunehmend vernetzten Welt noch gerecht wird, sollte und muss kritisch hinterfragt werden.[272]

Die Binarität der Verantwortlichkeit – entweder ist man Verantwortlicher oder nicht – erscheint zu simpel, da sie die komplexe und auch opake moderne Verarbeitungsrealität nur unzureichend abbilden kann.[273] Ebenso ist fraglich, ob Aufsichtsbehörden, aber auch Akteure selbst, überhaupt ihre eigene Verantwortlichkeit belastbar erkennen können. Denn viele Verarbeitungsszenarien finden nur noch arbeitsteilig mit verschiedenen Arten von Beteiligungsgraden und -phasen statt. Dabei ist häufig kein Weisungsverhältnis oder eine Aufgabendelegation,

---

[267] Der Zweck scheint vielmehr die Kompensation von fehlender Transparenz ggü. der betroffenen Person zu sein. In diese Richtung: *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 503 f.

[268] *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 503.

[269] Vgl. zum BDSG a.F.: *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 143.

[270] Im Gegensatz zur Negativ-Definition des Dritten.

[271] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 11. Vgl. a. *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 145.

[272] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 11 f. m.w.N.; *Alsenoy*, CLSR[28] (2012), 25, 28, 35 m.w.N.; *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 146; *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 457; vgl. zu grundsätzlichen Problemen: *Spiecker gen. Döhmann*, CR 2016, 698, 700 f.

[273] *Alsenoy*, CLSR[28] (2012), 25, 35 m.w.N. Vgl. zum Problem eines globalen Regelungsanspruchs bzw. eines hohen Abstraktionsgrades: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 18; *Simitis*, CR 1987, 602, 603, 605.

im Sinne einer Auftragsverarbeitung, erkennbar. Es findet vielmehr eine organisatorische Differenzierung und Spezialisierung der Tätigkeiten im Kontext von Verarbeitungen statt.[274] Ebenso sind Zwecke und Mittel der Verarbeitung häufig größtenteils vorbestimmt, gerade durch Plattformbetreiber und die von ihnen betriebene Infrastruktur. Es liegen nicht frei konfigurierbare Produkte vor, sondern häufig nur take-it-or-leave-Angebote.

Illustrativ für das Dilemma der soeben beschriebenen Binarität der Verantwortlichkeit ist folgendes Zitat von *Sartor* zur Frage, ob Suchmaschinenbetreiber als (für die Verarbeitung) Verantwortliche einzuordnen sind:

> *„Both approaches, I would argue, have some questionable implications: the first deprives the data subject of an effective protection; the second expands the data protection obligations of search engine operators to an extent that questions the very possibility for them to operate lawfully, and may push them into 'collateral censorship', namely, into removing even information that should be legally distributed, for avoiding the risk of punishment."*[275]

Die Forderung nach einer grundsätzlichen Revision des Datenschutzrechts ist nicht neu. Entsprechende Kritik wurde bereits 2000, noch vor Umsetzung der DSRL, geäußert.[276] Besonders das Gutachten zur „Modernisierung des Datenschutzrechts" im Auftrag des Bundesministeriums des Inneren aus dem Jahr 2001 äußerte umfassende Kritik am allgemeinen Schutzkonzept:[277]

> *„Das Datenschutzrecht ist vom Ansatz her orientiert an einer Datei personenbezogener Daten, die von einer verantwortlichen Stelle in einer zentralen Datenverarbeitungsanlage verarbeitet oder zu einer solchen übermittelt wird. Dieses Schutzkonzept ist in den 70er Jahren am Paradigma zentraler staatlicher Großrechner entwickelt worden, zwischen denen ein Datenaustausch die Ausnahme war.[278] Soweit seine Konstitutionsbedingungen*

[274] *Alsenoy*, CLSR[28] (2012), 25, 35 f. Vgl. Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 87 zu Problemen der Zuweisung der Verantwortlichkeit aufgrund der Dezentralisierung der Verarbeitung.

[275] *Sartor*, MJ[21] (2014), 564, 566.

[276] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 124 m.w.N.

[277] Überblicksartig: *Roßnagel*, 1. Einleitung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 25 ff.

[278] Vgl. a. *Roßnagel*, 1. Einleitung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 26.

> *noch fortbestehen, vermag das bisherige Konzept den Ansprüchen zu genügen. Soweit jedoch personenbezogene Daten in weltweiten Datennetzen von vielen Beteiligten ohne durchgreifende zentrale Kontrollmöglichkeiten verarbeitet werden, muss dieses Konzept als überholt gelten und durch neue konzeptionelle Maßnahmen ergänzt oder ersetzt werden."*[279]

Konkret für die Frage des Normadressaten:

> *„Für [die Datenverarbeitung] ist es nahezu ausgeschlossen, für alle relevanten Fälle den jeweils richtigen Adressaten der rechtlichen Regelung durch technische oder organisatorische Funktionsbeschreibung zu benennen."*[280]

Folgerichtig wurde bereits in diesem Gutachten die Ausweitung der Verantwortlichkeit auf Hersteller und Entwickler in gewissem Umfang gefordert.[281]

Unabhängig von spezifischen Problemen im Zusammenhang mit dem Konzept des Verantwortlichen zeigt sich also, dass allein aufgrund der technischen und gesellschaftlichen Entwicklung eine grundlegende Revision oder wenigstens Ausdifferenzierung der Verantwortlichkeit dringend überfällig ist.[282] Ob aufgrund der Verordnungsnatur der DSGVO aber langfristig noch Innovationen in den Mitgliedstaaten abseits von Brüssel und Straßburg zu erwarten sind, bleibt abzuwarten.[283]

---

[279] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 22. Ähnlich a. *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 78 speziell zur verantwortlichen Stelle.

[280] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 63.

[281] Dazu: Kapitel 5 G. Herstellerverantwortlichkeit. *Roßnagel*, 1. Einleitung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 46.

[282] .Anders noch die Art. 29-Datenschutzgruppe 2010: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11, 40.

[283] *Roßnagel*, DuD[36] (2012), 553, 553.

Kapitel 2

Definitionselemente des Verantwortlichen und Abgrenzung

> *„Die Rolle des für die Verarbeitung Verantwortlichen ergibt sich in erster Linie aus dem Faktum, dass eine Organisation entschieden hat, personenbezogene Daten für ihre eigenen Zwecke zu verarbeiten."*[1]

> *„Controllers are, roughly speaking, entities that hold personal data and decide what to do with it. [...] they are the decisionmakers [...]"*[2]

Mit diesen beiden Zitaten lässt sich die Essenz dessen, was einen Verantwortlichen ausmacht, nämlich die Entscheidung über die Verarbeitung personenbezogener Daten, gut beschreiben. Neben der Entscheidung sollen aber auch die anderen Elemente der Definition des Verantwortlichen in diesem Teil der Arbeit genauer untersucht werden. Dabei werden bestimmte Aspekte der Elemente, die gemeinsam Verantwortliche betreffen, bereits in diesem Abschnitt behandelt, um eine kohärente Darstellung zu wahren. Insgesamt wird die gemeinsame Verantwortlichkeit aber in Kapitel 4 behandelt.

Allgemein setzt Verantwortung drei Elemente[3] voraus: zunächst ein Verantwortungssubjekt, also denjenigen, dem eine Verantwortung zugeordnet wird. Daneben bedarf es eines Verantwortungsobjektes, also den- oder dasjenige für den oder das eine Verantwortung bestehen soll. Zuletzt muss noch ein Verantwortungsgrund bestehen, also eine Verbindung zwischen Verantwortungssubjekt und -objekt, die gleichermaßen auch Art und Ausmaß der Verantwortung bestimmt.[4] Im Rahmen der datenschutzrechtlichen Verantwortlichkeit ist das Verantwortungssubjekt der Verantwortliche, das Verantwortungsobjekt die Verarbeitung personenbezogener Daten und der Verantwortungsgrund die Entscheidung über die (Zwecke und Mittel der) Verarbeitung. Dabei kennt die Entscheidung über die Verarbeitung kein

---

[1] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[2] *Keller*, BTLJ[33] (2018), 287, 307.

[3] *Augsberg*, RW 2019, 109, 109 f.; *Eller*, RW 2019, 5, 14; vgl. zum Begriff Verantwortung insgesamt die Darstellung bei: *Klement*, Verantwortung, 2006, 202 ff.

[4] *Augsberg*, RW 2019, 109, 109 f.

Intensitätskriterium. Eine Abstufung der Verantwortung je nach Intensität eines Entscheidungsbeitrags erfolgt gerade nicht. Die Verantwortung für eine Verarbeitung ist also aufgrund der tatbestandlichen Ebene immer identisch im Ausmaß. Dies gilt neben den singulären auch für die gemeinsam Verantwortlichen. Eine Abstufung der Verantwortung kann sich allerdings gegenüber der Aufsichtsbehörde oder auf der Haftungsebene ergeben. Für eine Auftragsverarbeitung bleibt grundsätzlich der Verantwortliche verantwortlich, da die Verarbeitung in seinem Auftrag und somit seiner Verantwortung erfolgt. Abseits spezifischer normativer Anordnung[5] übernimmt der Auftragsverarbeiter nur dann selbst Verantwortung, wenn er den Rahmen seines Auftrags und damit seiner Weisungsgebundenheit verlässt.[6]

Eine der Kernfragen der datenschutzrechtlichen Verantwortlichkeit ist, wie die verschiedenen Arten bzw. Rollen der Verantwortlichkeit voneinander abzugrenzen sind. Sofern nur ein einzelner datenverarbeitender Akteur vorhanden ist, kann es sich bei diesem entweder um einen Verantwortlichen oder Auftragsverarbeiter[7] handeln. Sind zwei oder mehr verarbeitende Akteure vorhanden, kann es sich bei diesen um voneinander unabhängige, also singulär Verantwortliche handeln, es können gemeinsam Verantwortliche vorliegen oder aber ein Verantwortlicher und sein Auftragsverarbeiter. Die Einordnung der jeweiligen Rollen wird mit steigender Zahl der beteiligten Akteure immer komplizierter. Ausgangspunkt für eine jede Einordnung sollte zunächst immer die Bestimmung zumindest eines Verantwortlichen sein. Zwar ist eine Verarbeitung ohne Verantwortlichen prinzipiell denkbar, sie bildet aber die absolute Ausnahme.[8] Ausgehend von einem Verantwortlichen lassen sich in Relation zu diesem die Rollen der weiteren beteiligten Akteure bestimmen. So setzt ein Auftragsverarbeiter definitionsgemäß den Auftrag und damit die Präsenz eines Verantwortlichen voraus. Auch die Differenzierung zwischen Auftragsverarbeiter und gemeinsam sowie unabhängig Verantwortlichen setzt mindestens einen bereits erkannten Verantwortlichen voraus. Schließlich kann aber auch bei nur einem Akteur maßgeblich sein, wie weit dessen Verantwortlichkeitssphäre geht, etwa im Hinblick auf dessen Beschäftigte oder einen Auftragsverarbeiter. Daher sind die Voraussetzungen wie auch die damit einhergehende Verantwortlichkeitssphäre des Verantwortlichen

[5] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 51 mit einer Auflistung. Die DSRL kannte insgesamt noch keine Verantwortung des Auftragsverarbeiters: ebd., Rn. 4.

[6] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess. *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 52.

[7] Denn der Verantwortliche kann die Verarbeitung selbst an den Auftragsverarbeiter delegieren.

[8] Denkbar wäre insofern die Verarbeitung durch ein Kind (Dazu: Kapitel 2 E. II. Vorfrage: Entscheidungsfähigkeit) oder die Haushaltsausnahme (Dazu: Kapitel 5 I. Haushaltsausnahme). Anders: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 2, 224.

unabdingbare Grundlage für eine Analyse der Rollen verschiedener Akteure in datenschutzrechtlichen Szenarien.

Die maßgeblichen Definitionen des „Verantwortlichen" in Art. 4 Nr. 7 DSGVO und dessen Vorgängernorm, dem „für die Verarbeitung Verantwortlichen" in Art. 2 lit. d DSRL, sind nahezu identisch.[9] Auch wenn die Definition der „verantwortlichen Stelle" in § 3 Abs. 7 BDSG a.F. nicht dem Wortlaut der DSRL entsprach, musste sie dennoch unionsrechtskonform i.S.d. DSRL auslegt werden. Aufgrund der Einheitlichkeit dieser verschiedenen Definitionen wird in dieser Arbeit auch auf Rechtsprechung, aufsichtsbehördliche Stellungnahmen und Literatur vor Geltungsbeginn der DSGVO eingegangen. Daneben definiert die ePrivacy-RL den Verantwortlichen nicht gesondert. Sie verweist stattdessen in Art. 2 S. 1 ePrivacy-RL auf die Definitionen der DSRL, also via Art. 94 Abs. 2 S. 1 DSGVO auf die Definition der DSGVO.

Die DSGVO definiert den Verantwortlichen in Art. 4 Nr. 7 insgesamt wie folgt:[10]

> *„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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;"*

Zu dieser Definition lässt sich zunächst grundlegend anmerken, dass die Auslegung des Begriffs des Verantwortlichen unionsrechtsautonom erfolgen muss.[11] Rückschlüsse auf das Verständnis des Verantwortlichen, die sich allein aus dem deutschen (Datenschutz-)Recht und nicht auch aus dem Recht anderer Mitgliedstaaten ergeben, sind daher nicht angebracht.[12] Nach Ansicht der Art. 29-Datenschutzgruppe sollte darüber hinaus der Begriff des Verantwortlichen auch

[9] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 2 Fn. 11.

[10] Vgl. Art. 3 Nr. 8 DSRL-JI und Art. 3 Nr. 8 VO (EU) 2018/1725.

[11] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11; *Monreal*, CR 2019, 797, Rn. 17, 37; *Kremer*, CR 2019, 225, Rn. 2. Vgl. zur unionsrechtsautonomen Auslegung a. EuGH, Urteil vom 01.10.2019 – C-673/17 (Planet 49) = EuZW 2019, 916, Rn. 47 f.

[12] Anderes gilt für die allgemeinen Rechtsgrundsätze, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind, vgl. Art. 340 Abs. 2, 3 AEUV.

autonom von anderen Rechtsgebieten verstanden werden.[13] Der EuGH schließlich betont immer wieder, dass der Begriff des Verantwortlichen weit ausgelegt werden muss.[14]

Strukturell lässt sich von der eigentlichen Definition zunächst der zweite Halbsatz ausklammern. Dieser erlaubt eine Festlegung der Verantwortlichkeit durch das Unionsrecht oder das Recht der Mitgliedstaaten.[15] Die übrige Definition wird üblicherweise in drei oder vier unterschiedliche Elemente aufgespalten.[16] Diese sind:

- natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle (**personenbezogener Aspekt**)
- Zweck und Mittel der Verarbeitung (**Abgrenzungsaspekt**[17])
- entscheidet (**Abgrenzungsaspekt**)
- allein oder gemeinsam mit anderen (**Möglichkeit der „pluralistischen Kontrolle“**[18])

Zwecks einer genaueren Analyse der einzelnen Elemente wird die Definition des Verantwortlichen hier noch weiter aufgespalten.[19] Dazu werden die Zwecke und Mittel getrennt voneinander untersucht. Ebenso wird der Bezug des Verantwortlichen zur Verarbeitung isoliert betrachtet. Der personenbezogene Aspekt der Definition des Verantwortlichen wird unter dem Oberbegriff der Stelle zusammengefasst. Demnach sind die für diese Arbeit maßgeblichen Elemente der Definition:

- die **Stelle,**
- die **allein / gemeinsam mit anderen**
- über **Zwecke** und

[13] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 13.

[14] Zuletzt: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 66. M.w.N.: *Monreal*, CR 2019, 797, Rn. 37. So a.: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 14.

[15] Dazu: Kapitel 2 F. Benennung durch (materielles) Gesetz.

[16] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10 ff. Das WP 169 unterscheidet zwischen drei Elementen und zusätzlich einem grundlegenden Element. Ebenso: *Monreal*, CR 2019, 797, Rn. 24.

[17] Die Abgrenzung erfolgt ggü. den anderen Akteuren des Datenschutzrechts.

[18] Diese Bezeichnung verwendet *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10.

[19] Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 16, der fünf Elemente der Definition isoliert.

- über **Mittel**
- der **Verarbeitung**
- von **personenbezogenen Daten**
- **entscheidet.**

Die Definitionselemente „Verarbeitung“ und „personenbezogene Daten“ sind dabei nicht spezifischer Teil der Definition des Verantwortlichen, sondern definieren den Anwendungsbereich des Datenschutzrechts nach Art. 2 Abs. 1 DSGVO allgemein. Die Legaldefinition des Begriffs „Verarbeitung“ findet sich in Art. 4 Nr. 2 DSGVO, die der „personenbezogene[n] Daten“ in Art. 4 Nr. 1 DSGVO. Da der Begriff der „personenbezogene[n] Daten“ keine besonderen Probleme im Hinblick auf den Verantwortlichen aufwirft, wird auf die einschlägige Literatur und Rechtsprechung[20] hierzu verwiesen. Der Begriff der „Verarbeitung“ hingegen muss genauer analysiert werden, da die Verarbeitung Bezugspunkt der Entscheidung des Verantwortlichen ist. Da die Pflichten des Verantwortlichen an die jeweilige Verarbeitung anknüpfen, wird diese zuerst behandelt. Die weiteren Elemente der Definition des Verantwortlichen werden in der Reihenfolge ihres Auftretens untersucht. Ebenso wird der Auftragsverarbeiter zwecks Abgrenzung zum Verantwortlichen dargestellt.

A. Bezug zur Verarbeitung

Da der Verantwortliche definitionsgemäß über die (Zwecke und Mittel der) Verarbeitung[1] entscheiden muss, ist für eine Analyse des Verantwortlichen ein Verständnis des Begriffs der Verarbeitung notwendig.[2] Nach Art. 4 Nr. 2 DSGVO wird die Verarbeitung wie folgt definiert:[3]

[20] Zuletzt zum Personenbezug: EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328.

[1] Näher zu diesem mit der DSRL neu eingefügten Bezugsobjekt: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 10 ff.; Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 5 ff.; Ehmann/Helfrich DSRL, Art. 2, Rn. 27 ff.

[2] Zur Bedeutung der Verarbeitung für den Verantwortlichen: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 1; *Monreal*, CR 2019, 797, Rn. 14.

[3] Vgl. zum modernisierten Übereinkommen Nr. 108 des Europarates: BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 32a.

> *„‚Verarbeitung' jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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 Einschränkung, das Löschen oder die Vernichtung;"*

I. Verarbeitung als einheitlicher Begriff

Trotz der Auflistung einer Vielzahl von verschiedenen möglichen Formen einer Verarbeitung, handelt es sich bei der Verarbeitung in der DSGVO um einen einheitlichen Begriff. Die Darstellung der verschiedenen Formen ist nicht abschließend, wie das Wort „wie" verdeutlicht. Es gibt also keinen Typenzwang innerhalb der Verarbeitungsformen. Diese Herangehensweise steht im Widerspruch zur ursprünglichen Konzeption des BDSG und dem damit verbundenen Phasenmodell[4] der Verarbeitung, in dem besonders schutzbedürftige Phasen isoliert werden sollten.[5] Neben dem Begriff der Verarbeitung, der wiederum mehrere Unterphasen umfasste, enthielt das BDSG a.F. noch den Begriff des Erhebens[6] und des Nutzens[7]. Nutzen war jegliche Verwendung personenbezogener Daten, die keine Erhebung oder Verarbeitung darstellte. Somit bestand im BDSG a.F. kein einheitlicher Verarbeitungsbegriff, sondern eine Begriffs-Trias. Die DSGVO, wie auch vorher die DSRL, erfasst hingegen pauschal alle Formen der Verarbeitung aufgrund des einheitlichen Begriffs.[8] Im Gegensatz zu dem BDSG a.F. definiert die DSGVO nicht einzelne Phasen der Verarbeitung,[9] sondern zählt verschiedene denkbare Phasen[10] auf.

---

[4] Dazu: Kapitel 1 B. II. BDSG (1977). Eingehender: *Monreal*, PinG 2017, 216, 220; G/S/S/V/*Buchholtz/Stentzel*, Art. 4 Nr. 2 DSGVO, Rn. 2.

[5] So verhält sich BT-Drs. 14/4329, S. 33 (Umsetzung der DSRL) gar nicht zum Begriff der Verarbeitung. Siehe a. *Monreal*, CR 2019, 797, Rn. 19.

[6] § 3 Abs. 3 BDSG a.F.

[7] § 3 Abs. 5 BDSG a.F.

[8] Vgl. ErwGr 27 S. 2 DSRL; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 3; *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 151.

[9] Wie etwa § 3 Abs. 4 BDSG a.F.

[10] Der Begriff Phase war nicht ideal gewählt, da der Lebenszyklus personenbezogener Daten nicht notwendigerweise alle nach § 3 Abs. 4 BDSG a.F. definierten Phasen durchleben musste. Sinnvollerweise ver-

Der Verarbeitungsbegriff der DSGVO erfasst als dynamischer Begriff damit sämtliche Vorgänge in Bezug auf personenbezogene Daten.[11] Daher entfiel die für deutsche Juristen gewohnte Orientierung an spezifischen Phasen einer Verarbeitung. Es kommt für die Verantwortlichkeit nicht darauf an, welche Phase bzw. Form einer Verarbeitung vorliegt, sondern nur darauf, ob eine Verarbeitung überhaupt vorliegt. Eine Differenzierung verschiedener Formen einer Verarbeitung bleibt natürlich insoweit sinnvoll, wie damit verschiedene Verarbeitungsvorgänge unterschieden werden können.

II. Verarbeitung als einzelner Vorgang und Vorgangsreihe

Neben der Unterteilung in verschiedene Verarbeitungsphasen verwendete das BDSG a.F. in § 3 Abs. 4 S. 1 das Verb „Verarbeiten" und nicht die Substantivierung der „Verarbeitung". Diese Feststellung mag zunächst trivial klingen, allerdings konnte das BDSG a.F. damit sprachlich bedingt nur individuelle Verarbeitungsvorgänge ansprechen. Die DSGVO hingegen erfasst durch den Begriff der Verarbeitung nicht nur den einzelnen Verarbeitungsvorgang, sondern auch die Vorgangsreihe als Bündelung von Verarbeitungsvorgängen.[12] Eine vergleichbare Abstraktion war im BDSG a.F. allein schon aufgrund der Begriffs-Trias von Erheben, Verarbeiten und Nutzen kaum möglich. Zwar haben die Normen des BDSG a.F. seit Geltungsbeginn der DSGVO nur noch rechtshistorische Bedeutung, allerdings prägen diese historischen Definitionen bzw. die damit verbundene fehlerhafte Umsetzung der DSRL weiterhin das deutsche Verständnis des Begriffs der Verarbeitung.

Die Regulierung der Verarbeitung anhand verschiedener Phasen bzw. Vorgänge kann man als den „ausgefeiltesten Baustein des Datenschutzrechts" bezeichnen.[13] Auch

---

steht man eine bestimmte Phase der Verarbeitung als spezifische Form eines Verarbeitungsvorgangs. Ähnlich wohl a. der EuGH: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70, 72.

[11] Vgl. *Monreal*, CR 2019, 797, Rn. 18; *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 47.

[12] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5, 25. Hierzu a.: Kühling/Buchner/*Herbst*, Art. 4 Nr. 2 DS-GVO, Rn. 15; Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 22; S/J/T/K/*Schwartmann/Hermann*, Art. 2 DSGVO, Rn. 53. Verwunderlich ist daher, dass im Hinblick auf das Verarbeitungsverzeichnis aus Art. 30 DSGVO bei Kühling/Buchner/*Hartung*, Art. 30 DS-GVO, Rn. 14 f. zwecks Abstraktion kein Bezug zum Begriff der Vorgangsreihe hergestellt wird. Ebenso a.: *Kremer*, CR 2019, 225, Rn. 3.

[13] *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-

wenn die Regulierung der Verarbeitung sich, geprägt aus der Zeit der Großrechner, immer noch „als rechtliche Nachzeichnung faktischer Abläufe“ verstehen lässt,[14] begreift *Albers* sie als „problemorientierte Steuerung von Verarbeitungsphasen“. So soll die Verarbeitung einerseits isoliert, andererseits im jeweiligen Verarbeitungskontext und -prozess betrachtet werden.[15] Insgesamt soll zwischen phasenübergreifenden und phasenbezogenen Elementen unterschieden werden.[16] Dieses Verständnis der Verarbeitung lässt sich in der DSGVO dadurch abbilden, dass neben dem einzelnen Vorgang (phasenbezogen) auch die Vorgangsreihe (phasenübergreifend) erfasst wird.[17] Übergreifende Elemente sollen sich nach *Albers* auf alle Phasen beziehen und begrenzte und strukturierte Verarbeitungszusammenhänge herstellen. Phasenbezogene Elemente reagieren zusätzlich auf bestimmte Regelungsprobleme.[18] In Bezug auf die Zwecke[19] und Mittel[20] der Verarbeitung lässt sich diese Differenzierung wie folgt umsetzen:[21]

Elemente der Vorgangsreihe (phasenübergreifend):

- Zwecke
- Dauer der Verarbeitung (Speicherung, Löschung)
- Zugang zu den Daten

Elemente des einzelnen Vorgangs (phasenbezogen):

- Auswahl der Daten
- technische und organisatorische Fragen[22] (Verfahren)

Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, ²2012, Rn. 121.

[14] *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, ³2022, Rn. 82.

[15] *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, ³2022, Rn. 82.

[16] Also (verarbeitungs-)vorgangsübergreifenden und vorgangsbezogenen Elementen.

[17] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5.

[18] *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, ³2022, Rn. 82.

[19] Dazu: Kapitel 2 C. Zweck(e).

[20] Dazu: Kapitel 2 D. Mittel.

[21] Bei allen Elementen außer den Zwecken handelt es sich um Unterpunkte der Mittel.

[22] *Schreiber*, ZD 2019, 55, 55 erkennt dann eine Vorgangsreihe, die mehrere Vorgänge beinhaltet, wenn diese identische Zwecke und Mittel aufweisen. Sie wendet damit die gleichen Kriterien zur Bestimmung einer Vorgangsreihe an, die sie a. zur Bestimmung gemeinsam Verantwortlicher verwendet. Konsequenz wäre, dass auf verschiedene Vorgänge keine unterschiedlichen Verarbeitungsverfahren angewendet werden könnten, ohne dass der Charakter einer Vorgangsreihe entfallen würde.

Dabei ist die Zwecksetzung[23] der zentrale, phasenübergreifende Baustein für eine Regulierung der Verarbeitungsphasen bzw. der Vorgangsreihen.[24] Ein ähnliches Verständnis findet sich auch bei *Brühann*, der für die Vorgangsreihe explizit auf den übergreifenden Zweck hinweist.[25] Die anderen Elemente spielen daneben eine untergeordnete Rolle und bewirken insbesondere keine Verklammerung verschiedener Vorgänge. Gleichwohl wird die Entscheidung über die Dauer der Verarbeitung und über den Datenzugriff regelmäßig auf Ebene der Vorgangsreihe und nicht auf der Ebene einzelner Vorgänge fallen. Die einzelnen Elemente einer Vorgangsreihe lassen sich wiederum unproblematisch auf den einzelnen Vorgang als Teilmenge herunterbrechen.

Auch der EuGH hat im Urteil zu der Rechtssache Fashion ID[26] die Bedeutung der Differenzierung der individuellen Verarbeitungsvorgänge betont.[27] Nähere Ausführungen hierzu erfolgen kontextbezogen in Kapitel 2 C.[28] sowie Kapitel 4 L. II.[29].

Das Konzept der Vorgangsreihe lässt sich anhand eines Beispiels illustrieren. In diesem Beispiel solle eine Rechnung, die bislang nur analog vorhanden ist, per E-Mail zwecks Erstattung übermittelt werden. Mittels des Konzepts der Vorgangsreihe kann die Erhebung der Daten durch Scannen, die Speicherung der Daten im Gerät und die anschließende Übermittlung der Daten per E-Mail als Vorgangsreihe mit dem Zweck der Erstattung gebündelt werden. Nach dem Phasenmodell des BDSG a.F. hingegen musste jeder Vorgang einzeln erfasst und der entsprechenden Form der Verarbeitung zugeordnet werden.

Der Europäische Datenschutzbeauftragte (European Data Protection Supervisor, im Folgenden „EDPS“)[30] geht in seinen Guidelines zum Verantwortlichen davon aus, dass sowohl einzelne Vorgänge wie auch Vorgangsreihen der Kontrolle eines Verantwortlichen und somit seiner Verantwortung unterliegen können.[31] Zwar sei bei

---

[23] Bzw. die Zweckfestlegung in Abgrenzung zur nachgelagerten Zweckbindung.

[24] *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 123; vgl. a. *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, [3]2022, Rn. 83.

[25] Mit Verweis auf die Meldung nach Art. 18 Abs. 1 DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 12. Kritisch hingegen: *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 107 ff.

[26] Dazu: Kapitel 4 B. III. Fashion ID.

[27] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74.

[28] Dazu: Kapitel 2 C. Zweck(e).

[29] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[30] Im Deutschen ist auch die Abkürzung „EDSB“ üblich. Die Rechtsgrundlage für den Beauftragten findet sich in Art. 52 VO (EU) 2018/1725.

[31] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and

einer wörtlichen Auslegung der DSGVO jede einzelne Handlung im Zusammenhang mit personenbezogenen Daten eine separate Verarbeitung. In der Praxis würden solche einzelnen Vorgänge allerdings als Vorgangsreihen mit einheitlichen Zwecken zusammengefasst. Dabei sollen die Verantwortlichen im Hinblick auf die Festlegung der Grenzen der Vorgangsreihen über einen gewissen Ermessensspielraum verfügen. Verantwortliche sollen zudem bei der Beurteilung der Frage, ob es sich um einzelne Vorgänge oder vielmehr um Vorgangsreihen handelt, vor allem die Perspektive der betroffenen Personen berücksichtigen.[32]

Inwiefern ist die Differenzierung zwischen einzelnem Vorgang und Vorgangsreihe nun für das Verständnis des Verantwortlichen maßgeblich? Zum einen können anhand der Zwecke verschiedene Vorgänge zu einer Vorgangsreihe zusammengefasst werden.[33] Die Zweckfestlegung bildet als Voraussetzung der Zweckbindung einen der Grundsätze der Verarbeitung personenbezogener Daten gem. Art. 5 Abs. 1 lit. b DSGVO und strukturiert die Pflichten des Verantwortlichen. Die Vorgangsreihe dient also der Rationalisierung und Strukturierung der Verarbeitung. So können beispielsweise die verschiedenen Verarbeitungsvorgänge, die zur Berechnung einer Route durch eine Navigationsapp notwendig sind, zusammengefasst werden. Zum anderen kann anhand der Differenzierung unterschiedlicher Vorgänge und Vorgangsreihen auch die Verantwortlichkeit und damit verbunden die Wahrnehmung der Pflichten und Haftung zwischen verschiedenen Akteuren wie etwa Verantwortlichem und Auftragsverarbeiter, vor allem aber zwischen gemeinsam Verantwortlichen, sinnvoll begrenzt werden.[34]

B. Stelle

Das scheinbar unproblematischste Definitionselement des Verantwortlichen ist die Stelle.[35] Auch wenn die Definition des Verantwortlichen neben der Stelle ebenso noch die natürliche oder juristische Person, die Behörde und die Einrichtung erwähnt, kann man die Stelle als Auffang- und damit auch Überbegriff zu den anderen Subjekten

joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 11. Ebenso: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 42.

[32] Berücksichtigt werden soll also, ob es sich bei den fraglichen Vorgängen um einen integrierten Prozess handelt. Gemeint ist wohl ein einheitlicher Prozess.

[33] Dazu: Kapitel 2 C. Zweck(e).

[34] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[35] Die englischsprachige Entsprechung ist „body".

verstehen („[...] oder jede andere Stelle, [...]“).[36] In dieser Funktion ist die Stelle eine weitestgehend unspezifizierte Organisationseinheit.[37] Der Unionsgesetzgeber knüpft, abseits der natürlichen Person, nicht an eine einzelne Person, sondern grundsätzlich an solche Organisationseinheiten an. Die Stelle als Definitionselement entspricht fast wörtlich dem Übereinkommen Nr. 108 des Europarates[38] und war nicht Gegenstand von Diskussionen im Gesetzgebungsprozess zur DSRL[39] oder zur DSGVO. Im modernisierten Übereinkommens Nr. 108 des Europarates[40] wird in Art. 2 lit. d zusätzlich noch „service“[41] erwähnt. Der Explanatory Report zum Übereinkommen verhält sich zu diesem Begriff allerdings nicht.[42] Systematisch liegt es nahe, dass mit „service“ eine spezifische Variante einer öffentlichen Stelle gemeint ist.

Auch wenn es sich bei der Stelle um ein scheinbar einfaches Definitionselement handelt,[43] sollte seine Bedeutung nicht unterschätzt werden. Über die Konturierung der Stelle bestimmen sich einerseits das anwendbare Recht, andererseits auch die für die Verarbeitung privilegierten Personen nach Art. 29 DSGVO.[44] Daneben wird die Konturierung der Stelle auch für das Verhängen von Sanktionen nach Art. 83 f. DSGVO sowie für die Haftung nach Art. 82 DSGVO relevant.[45]

---

[36] Ähnlich wie die Definition der Verarbeitung in Art. 4 Nr. 2 DSGVO verschiedene Varianten der Verarbeitung aufzählt.

[37] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 17. Vgl. zur Definition in Art. 3 Nr. 7 VO (EU) 2018/1725: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 7. Ähnlich zur Definition des Dritten in der DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 23: „[...] jede Person im weiteren Sinne einer rechtlichen Einheit [...]“.

[38] Art. 2 lit. d Übereinkommen Nr. 108 des Europarates.

[39] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19.

[40]. Council of Europe, Nr. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223.

[41] Flankiert von „public authority“ und „agency“.

[42] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 22.

[43] *Monreal*, CR 2019, 797, Rn. 25 etwa problematisiert es überhaupt nicht.

[44] Für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 20.

[45] Dazu: Kapitel 3 C. Die Verhängung von Geldbußen und Kapitel 3 A. Haftung auf Schadensersatz. Für die DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20.

I. Verständnis der Aufsichtsbehörden[46]

Die Art. 29-Datenschutzgruppe wollte die Stelle in ihrem WP 169 so ausgelegt wissen, dass eine möglichst eindeutige Bestimmung des Verantwortlichen, unabhängig von einer „formalen Benennung", erfolgen kann.[47] Die Bestimmung der Stelle solle sich an der üblichen Rechtspraxis im öffentlichen und privaten Sektor (also etwa Zivil-, Verwaltungs- und Strafrecht) orientieren, da dort regelmäßig Personen und Stellen Verantwortlichkeit zugewiesen werde. Dies könne auch bei der Bestimmung der Stelle i.S.d. Verantwortlichen helfen. So sei ein Rückschluss von einer zivilrechtlichen Haftung auf eine Stelle grundsätzlich unproblematisch. Allerdings würden einige Mitgliedstaaten keine verwaltungs- oder strafrechtliche Haftung juristischer Personen kennen. In diesem Fall hafte eventuell dann der Funktionsträger der juristischen Person.

Nur ausnahmsweise, bei klaren Anzeichen hierfür, solle eine natürliche Person als Verantwortlicher angenommen werden. [48] Der Grundsatz sei vielmehr, dass eine Behörde oder ein Unternehmen einen Verantwortlichen darstelle.[49] Auch eine spezifische Abteilung oder eine Einheit einer Organisation, die in operativer Hinsicht für bestimmte Verarbeitungen verantwortlich ist, solle grundsätzlich nicht selbst als Verantwortlicher gelten.[50] Generell solle vielmehr gelten, dass eine öffentliche Einrichtung oder ein Unternehmen für Verarbeitungen in ihrem jeweiligen Tätigkeits- und Haftungsbereich verantwortlich sei. Ausnahmsweise sei eine natürliche Person, die für eine juristische Person handele,[51] dann Verantwortliche, wenn sie Daten für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle der juristischen Person verarbeite.[52] Die natürliche Person werde damit selbst zum

[46] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19 ff.

[47] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19.

[48] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19.

[49] Ähnlich: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 17.

[50] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 18 mit Beispiel.

[51] Also beispielsweise der Mitarbeiter eines Unternehmens.

[52] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20. Da die Art. 29-Datenschutzgruppe offensichtlich öffentliche Einrichtungen (wohl auch Behörden) als juristische Personen begreift (ebd., 21), gelten diese Erwägungen allerdings a. für natürliche Personen in Behörden.

Verantwortlichen und hafte entsprechend.[53] Allerdings könne in Ermangelung entsprechender Sicherheitsmaßnahmen auch den ursprünglich Verantwortlichen eine gewisse Verantwortlichkeit treffen.[54]

II. Eindeutige Bestimmung der Stelle in ihren verschiedenen Formen?

Die Bestimmung der Stelle in ihren unterschiedlichen Varianten ist nicht durchweg unproblematisch. Einfach ist die Bestimmung etwa noch bei der natürlichen Person. Diese ist hinsichtlich ihrer personellen und organisatorischen Grenze klar konturiert. Allerdings wird bei natürlichen Personen als Stellen im Hinblick auf die Haftung sowie Sanktionierung nach Art. 82 f. DSGVO teilweise zusätzlich eine Rechts- und Prozessfähigkeit gefordert.[55] Da die Rechts- und Prozessfähigkeit natürlicher Personen aber je nach Mitgliedstaat variieren kann, ist es hier sinnvoller auf ein unionsrechtsautonomes Verständnis von Entscheidungsfähigkeit abzustellen.[56] Wäre also beispielsweise ein Kind nicht rechts- oder prozessfähig, könnte auf seine Fähigkeit, die Entscheidung über die Verarbeitung zu überblicken, abgestellt werden. Die Haftung sowie Sanktionierung könnten dann über die gesetzlichen Vertreter des Kindes erfolgen.

Auch die Konturierung juristischer Personen sollte weitestgehend unproblematisch möglich sein. Bei der Auslegung des Begriffs der juristischen Person ist ebenso ein unionsrechtliches Verständnis maßgeblich. Demnach können juristische Personen alle Stellen sein, denen das Völker-, Unions- oder mitgliedstaatliche Recht Rechte oder Pflichten zuweist.[57] Ob es sich beim Gründungsakt der juristischen Person um einen des öffentlichen Rechts oder des Privatrechts handelt, ist unerheblich.[58] Juristische Personen im Privatrecht wären etwa die GmbH, die AG oder OHG, im öffentlichen Bereich wären damit etwa öffentlich-rechtliche Unternehmen sowie Personal- und Gebietskörperschaften erfasst.

Die Erwähnung der Behörde in der Definition des Verantwortlichen macht nur Sinn, wenn man diese anders als eine öffentlich-rechtliche juristische Person konturiert.

---

[53] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[54] Dabei wird allerdings nicht klar, für welche Vorgänge diese „gewisse Verantwortung" bestehen soll und ob diesbezüglich eine gemeinsame Verantwortlichkeit vorliegen kann.

[55] Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 128.

[56] Dazu: Kapitel 2 E. II. Vorfrage: Entscheidungsfähigkeit.

[57] Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 129. Möglicherweise erfolgt damit a. eine Zuordnung der bei *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 42 genannten Stellen.

[58] Anders für das BDSG a.F.: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 16.

Demnach kann der Rechtsträger, anders als etwa für die Bestimmung des Klagegegners in § 78 Abs. 1 Nr. 1 VwGO, als Organisationseinheit nicht maßgeblich sein.[59] Ansonsten würde die Übermittlung zwischen verschiedenen Behörden eines Rechtsträgers aufgrund einer einheitlichen Stelle i.S.v. Art. 29 DSGVO privilegiert. Da die DSGVO aber kein Konzernprivileg kennt, wäre es nicht schlüssig für öffentliche Stellen dennoch ein Rechtsträgerprinzip anzunehmen. Der EuGH hat zudem bereits entschieden, dass Behörden, Einrichtungen und Stellen nicht zwingend eine Rechtspersönlichkeit benötigen.[60] Sinnvoll ist es daher den Begriff der Behörde funktionell zu verstehen.[61] Die Behörde muss also aufgrund ihres Aufgabenbereichs abgrenzt werden können und eine gewisse Entscheidungsautonomie genießen.[62] Diese Entscheidungsautonomie sollte sich jedenfalls auf die Zwecke oder die wesentlichen Elemente der Mittel[63], insbesondere die Auswahl der verarbeiteten Daten, beziehen. Externe Vorgaben betreffend die technischen und organisatorischen Elemente der Mittel, etwa aufgrund einer zentralen technischen Infrastruktur, sind unschädlich. Nicht als separate Behörden anzusehen sind allerdings einzelne Abteilungen, Referate, Dezernate oder Sachgebiete.[64] Organisatorisch verantwortlich für diese ist vielmehr der Behördenleiter bzw. das Leitungsgremium.[65] Neben der Abgrenzbarkeit einer Behörde aufgrund ihres Aufgabenbereichs und ihrer Entscheidungsautonomie ist zudem maßgeblich, inwiefern in ihr eine Organisationseinheit aus Sicht der betroffenen Person erkannt werden kann. So ist etwa die örtliche Bauaufsichtsbehörde als Behörde zu erachten, ebenso das örtliche Polizeipräsidium an Stelle einer regionalen Übergliederung.[66] Hinsichtlich der Abgrenzbarkeit einer Behörde hat der EuGH bereits in einem umstrittenen Urteil festgehalten, dass auch der Petitionsausschuss eines

[59] Unklar: Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 129.

[60] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265, Rn. 36. Vgl. a. Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 16.

[61] Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 130; Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 19; BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 110 f. Vgl. a. Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 149 Fn. 16 und Update Mai 2021, 37; G/S/S/V/*Kramer*, Art. 4 Nr. 7 DSGVO, Rn. 17 will ihn organisatorisch verstehen. Für das BDSG a.F.: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 19.

[62] Einzelne Beispiele finden sich in ErwGr 31 DSGVO.

[63] Dazu: Kapitel 2 D. Mittel.

[64] Vgl. für das BDSG a.F. *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 20. Ausnahmsweise könnten aber a. diese Verantwortliche sein: Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 149 Fn. 18.

[65] Vgl. *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 22.

[66] Vgl. Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 12.

deutschen Landtages unter den Behördenbegriff der DSGVO fällt.[67] Eine genaue Begründung ist er dabei allerdings schuldig geblieben.[68] Insgesamt ist die Behörde i.S.d. der DSGVO daher als abgrenzbare Organisationseinheit anzusehen, die eine öffentliche Aufgabe mit Hoheitsgewalt durchführt.

Die Abgrenzung einer Einrichtung von einer Behörde ist bislang unklar.[69] Denkbar ist es für die Einrichtung auf die fehlende Hoheitsgewalt einer öffentlichen Stelle[70] abzustellen, die gleichsam aber über die Verarbeitung von personenbezogenen Daten entscheidet.[71]

Insgesamt hängt die Bestimmung von Behörden und Einrichtungen als Verantwortliche davon ab, wie viel Autonomie diese gegenüber den ihnen übergeordneten Strukturen im Hinblick auf die Entscheidung über die Verarbeitung genießen.[72] Im Zweifel ist davon auszugehen, dass nicht einzelne Teile einer Organisationseinheit, bspw. Untergliederungen einer Behörde, eine Stelle darstellen, sondern die Stelle die gesamte Organisationseinheit einschließt.[73] Die Art. 29-Datenschutzgruppe begründete dies mit der erforderlichen Transparenz gegenüber den betroffenen Personen.[74]

III. Person und Stelle als gegensätzliche Oberbegriffe

Teilweise wird in der Literatur vertreten, die „Person" sei Oberbegriff für nicht-öffentliche Adressaten, die „Stelle" hingegen sei Oberbegriff für öffentlich-rechtliche Adressaten der DSGVO.[75] Diese Differenzierung lässt sich dem Wortlaut der DSGVO

---

[67] EuGH, Urteil vom 09.07.2020 – C-272/19 (VQ/Hessen) = NVwZ 2020, 1497, Rn. 71. Vgl. hierzu BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 93d ff.

[68] „Zwar sind die Tätigkeiten des Petitionsausschusses des Hessischen Landtags zweifellos behördlicher Art [...]".

[69] G/S/S/V/*Kramer*, Art. 4 Nr. 7 DSGVO, Rn. 17 sieht nur eine Auffangfunktion.

[70] Zu diesem Begriff, der außerhalb der Definition von Art. 4 Nr. 7 DSGVO Verwendung findet: Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 132.

[71] So wohl Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 131, der allerdings Einrichtung und Stelle als Begriff zusammenzieht und die Stelle nicht als Oberbegriff versteht. Zu denken wäre etwa an die Rechnungshöfe.

[72] Allgemein zur Bestimmung der Verantwortlichkeit für die DSRL: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 20.

[73] So für die DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19; für das BDSG a.F.: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 225.

[74] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19.

[75] So Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 11 f. Anders: *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 9 ff. für das BDSG 2001.

nicht unbedingt entnehmen.[76] Im ursprünglichen Vorschlag der Kommission zur DSRL war die Rede von einer „[...] Person, Behörde, Dienststelle oder jede[r] andere[n] Einrichtung [...]".[77] In den Erläuterungen zum abgeänderten Vorschlag der Kommission wurde nur eine „Person, die [...] verantwortlich ist", erwähnt.[78] Allerdings erfolgte diese Ausführung vor allem im Zusammenhang mit der Abkehr vom Begriff des „Verantwortliche[n] der Datei", um zu einem organisationsbezogenen Verständnis des Verantwortlichen zu gelangen.[79] Daneben wurde im Rahmen des Gesetzgebungsverfahrens zur DSRL bewusst die formelle Unterscheidung zwischen den für den öffentlichen und den für den privaten Sektor geltenden Normen aufgegeben.[80] Auch das WP 169 der Art. 29-Datenschutzgruppe sprach im Hinblick auf diesen Teil der Definition nur insgesamt vom „personenbezogenen Aspekt der Definition".[81] Denkt man diese Differenzierung zwischen Person und Stelle konsequent weiter, wären die Personen abschließend aufgezählt, die Stellen hingegen im Rahmen des „[...] oder andere Stelle [...]" nicht.[82] Eine solche Schlussfolgerung könnte Konsequenzen haben im Hinblick auf die Schaffung weiterer Personen neben der natürlichen und juristischen Person, etwa einer „elektronischen Person".[83] Gerade weil die DSGVO aber Stellen teilweise explizit als öffentlich qualifiziert,[84] ist es sinnvoll, den Begriff der Stelle insgesamt als Oberbegriff zu verstehen.[85] Daneben ist einer solchen Differenzierung zwischen Personen und Stellen ohnehin nicht viel Relevanz beizumessen. So wäre eine juristische Person als Unterfall der Person ebenso eine nicht individuumsbezogene Zuordnungseinheit wie auch die öffentlichen Stellen.

[76] So könnte man nach ErwGr 25 DSRL den Begriff der Stelle a. als allgemein übergeordneten Begriff verstehen, je nachdem worauf sich das „anderen für die Verarbeitung verantwortlichen Stellen" bezieht, also nur die Geschäftsstellen oder die anderen aufgezählten Subjekte.

[77] BR-Drs. 690/90, S. 52 f.

[78] BT-Drs. 12/8329, S. 13 f.

[79] Die Erläuterungen enthalten das Beispiel des Betriebsleiters.

[80] Siehe BT-Drs. 12/8329, S. 5; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 2.

[81] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10, 19.

[82] Vgl. zur öffentlichen Stelle als Oberbegriff zur Behörde: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 28 DSRL, Rn. 5.

[83] Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)).

[84] Etwa in Art. 37 Abs. 3 DSGVO.

[85] Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 131.

IV. Zurechnung des Verhaltens unterstellter Personen

Unklar ist im Detail, wie das Verhalten einzelner natürlicher Personen einer Stelle, die keine natürliche Person darstellt, zugerechnet wird. Teilweise greifen die deutschen Aufsichtsbehörden auf den funktionalen Unternehmensbegriff in ErwGr 150 S. 3 DSGVO i.V.m. Art. 101 und 102 AEUV zurück.[86] Dieser funktionale Unternehmensbegriff, der eigentlich im Zusammenhang mit der Bemessung von Geldbußen steht, knüpft nicht strikt an das Gesellschaftsrecht an. Als Unternehmen wird die wirtschaftliche Einheit aller Teile des Unternehmens und auch rechtlich selbstständiger Konzernunternehmen angesehen. Aus dem funktionalen Unternehmensbegriff soll auch die Anwendung des allgemeinen Funktionsträgerprinzips folgen. Danach werden auch einzelne Personen als Teil des Unternehmens betrachtet, wenn sie für das Unternehmen wirtschaftlich tätig sind. Die konkrete arbeits- oder vertragsrechtliche Beziehung des Unternehmens zur tätigen Person ist dann unerheblich. Ein bestimmender Einfluss auf die tätige Person seitens der Unternehmensleitung ist ausreichend.

Ob dieser Rückgriff aber überhaupt nötig ist, erscheint eher fraglich. Die DSGVO grenzt die Verantwortungssphären einzelner Stellen über die Definition des Dritten gem. Art. 4 Nr. 10 DSGVO ab.[87] Aufgrund der Negativdefinition des Dritten sind alle, außer den dort genannten Stellen, Dritte. Dies allein klärt allerdings noch nicht, wann die Grenze zu einer Zuordnung zum Verantwortlichen überschritten ist. Im Gegensatz zum Auftragsverarbeiter regelt die DSGVO die dem Verantwortlichen unterstellten Personen[88] nur rudimentär. Allerdings ergibt sich aus Art. 29 DSGVO, dass eine Zuordnung jedenfalls dann nicht mehr möglich ist, wenn sich die dem Verantwortlichen unterstellte Person entgegen der Weisung, abgesehen von unions- oder mitgliedstaatlicher Verpflichtung, des Verantwortlichen (oder Auftragsverarbeiters) verhält.[89] Ebenso ist in entsprechender Anwendung von Art. 28 Abs. 10 DSGVO auch dann eine Zuordnung nicht mehr möglich,[90] wenn die unterstellte Person eigenmächtig über die Zwecke und Mittel der Verarbeitung

[86] So jedenfalls: *Ambrock*, ZD 2020, 492, 493.

[87] Vgl. *Piltz*, https://www.delegedata.de/2020/10/der-dritte-nach-der-dsgvo/ (abgerufen am 17.07.2024).

[88] „ [...] und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;“ (Art. 4 Nr. 10 DSGVO). „ [...] und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat [...]“ (Art. 29 DSGVO).

[89] Ausführlich hierzu: *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 52 ff.

[90] Die analoge Anwendung stellen unter anderem die bayrischen Datenschutzaufsichten BayLfD und BayLDA in Frage: BayLDA, 9. TB 2019, S. 71 f.

entscheidet und somit selbst zum Verantwortlichen wird.[91] Abgesehen von diesen systematischen Argumenten erschließt sich auch aus rechtshistorischer Perspektive die Notwendigkeit des Rückgriffs auf den funktionalen Unternehmensbegriff aus Art. 101 und 102 AEUV nicht. Diese Möglichkeit besteht erst seit Geltungsbeginn der DSGVO. Die DSRL kannte keinen vergleichbaren Erwägungsgrund zu ErwGr 150 S. 3 DSGVO.

Abzugrenzen vom Auftragsverarbeiter sind die dem Verantwortlichen gem. Art. 29 DSGVO unterstellten Personen insoweit, als dass sie dem Verantwortlichen gegenüber nicht nur im Hinblick auf bestimmte Verarbeitungen weisungsgebunden sind, sondern in grundsätzlicherer Natur weisungsgebunden sind. Dies kann sich aufgrund vertraglicher aber auch aufgrund gesetzlicher Weisungsgebundenheit ergeben. Regelmäßig wird es sich bei den unterstellten Personen um Beschäftigte des Verantwortlichen handeln. Aber auch Personen, die in vergleichbarer Weise in die Organisation des Verantwortlichen integriert sind, können als unterstellte Personen gelten. Maßgebliches Abgrenzungskriterium zum Auftragsverarbeiter ist damit der Integrationsgrad. Daneben wird der Auftragsverarbeiter auch regelmäßig nicht eine einzelne Person, sondern eine Organisationseinheit darstellen. Maßgeblich für die Zuordnung zum Verantwortlichen als unterstellte Person ist insgesamt also, dass diese Person weisungsgebunden gegenüber dem Verantwortlichen ist und gleichzeitig nicht einen Auftragsverarbeiter oder Dritten darstellt.

V. Der Konzern als Stelle?

Bei öffentlichen Stellen wie Behörden oder Einrichtungen ist deren Entscheidungsautonomie aufgrund der gesetzlichen Vorgaben grundsätzlich transparent. Sie können also vergleichsweise problemlos als individuelle Stellen identifiziert werden Die Feststellung, wo bei juristischen Personen Entscheidungsautonomie vorliegt, insbesondere im nicht-öffentlichen Bereich bei Konzernstrukturen,[92] ist hingegen nicht trivial.[93] So lässt sich erwägen, ob eine individuelle Tochtergesellschaft in einem Konzern noch eine abgrenzbare Stelle darstellt, soweit die Muttergesellschaft die tatsächliche Entscheidungsmacht innehat. Diese Fragestellung lässt sich auch hinreichend davon abgrenzen, inwieweit die

[91] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[92] Bzw. Unternehmensgruppen gem. Art. 4 Nr. 19 DSGVO.

[93] Vgl. die Empfehlungen der Art. 29-Datenschutzgruppe zu einer „Datenschutzstrategie“: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19 f. Vgl. a. BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 112 ff.

wirtschaftliche Einheit i.S.v. Art. 101 und 102 AEUV bei der Bemessung von Bußgeldern maßgeblich ist.[94]

Wie schwierig die Feststellung der Entscheidungsmacht ist, beweisen etwa die Vorlagefragen des BVerwG an den EuGH in der Rechtssache Wirtschaftsakademie.[95] In diesem Fall ging es um die Verarbeitung personenbezogener Daten mittels der Cookies eines Social-Media-Plattformanbieters und inwiefern ein Nutzer der Plattforminfrastruktur[96] hierfür gemeinsam (mit-)verantwortlich ist.[97] Eine Bildungseinrichtung (Wirtschaftsakademie Schleswig-Holstein) hatte auf einer Plattform eine Seite eingerichtet, um ihre Tätigkeiten zu bewerben. Sobald die Seite dieser Bildungseinrichtung auf der Plattform durch Besucher aufgerufen wurde, wurden personenbezogene Daten durch den Plattformanbieter verarbeitet. Der Plattformanbieter (Facebook) gliederte sich in eine US-amerikanische Muttergesellschaft (Facebook Inc.), eine irische Tochtergesellschaft (Facebook Ireland Ltd.) sowie eine deutsche Tochtergesellschaft (Facebook Germany GmbH). Nach Auffassung des Plattformanbieters sollte die irische Tochtergesellschaft konzernintern die ausschließliche Verantwortung für die Verarbeitungen im gesamten Gebiet der Union tragen, während die deutsche Tochtergesellschaft nur das Werbegeschäft betreue.[98] Die am Rechtsstreit beteiligte Aufsichtsbehörde machte allerdings geltend, dass die Entscheidung über die Verarbeitung, wie auch die Verarbeitung selbst, nicht durch die irische Tochtergesellschaft erfolge, sondern die Daten der im Unionsgebiet wohnhaften Nutzer an Server der Muttergesellschaft übermittelt und dort verarbeitet würden.[99] Das BVerwG hatte dem EuGH dann die Frage vorgelegt, unter welchen Voraussetzungen eine (von mehreren) Niederlassungen eines außerhalb der Union ansässigen Mutterkonzerns als Verantwortlicher angesehen werden könne. So sei fraglich, ob es ausreiche, dass sich die irische Niederlassung selbst als Verantwortliche bezeichne, auch wenn physikalisch die Datenverarbeitung ganz oder teilweise vom Mutterkonzern außerhalb des Unionsgebiets durchgeführt und maßgeblich von diesem gesteuert werde.[100] Würde dies ausreichen, käme es auf die Einzelheiten der

[94] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 57.

[95] Noch zur DSRL: BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 438 Vorlagefrage 3.

[96] Also nicht ein purer Nutzer der Plattform, vgl. EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 35.

[97] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 14 ff.

[98] Dies galt a. auf formeller Ebene aufgrund der Verträge mit den Nutzern. Siehe zur Delegation von Verantwortlichkeit: Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 223 ff.

[99] Mit Verweis auf EuGH, Urteil vom 06.10.2014 – C-362/14 (Schrems) = NVwZ 2016, 43, Rn. 27.

[100] BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, Rn. 39.

konzerninternen Entscheidungs- und Datenverarbeitungsstrukturen nicht mehr an. Würde die eigene Zuschreibung der Verantwortlichkeit hingegen nicht ausreichen, könnte auch eine andere Niederlassung des Mutterkonzerns (etwa die deutsche) als Verantwortliche angesehen werden. Diese könnte dann einer Aufsicht unterliegen, wenn die Datenverarbeitung tatsächlich nicht im Gebiet der Gemeinschaft erfolge. In diesem Fall seien vom nationalen Gericht zur Bestimmung der verantwortlichen Niederlassung zunächst die Einzelheiten der konzerninternen Entscheidungs- und Datenverarbeitungsstrukturen aufzuklären.

Die Kernfrage des BVerwG war also, ob die formelle Zuschreibung der Verantwortlichkeit für die Zuständigkeitsbegründung der Aufsichtsbehörde ausreicht. Für den Fall, dass dem nicht so sein sollte, schien das BVerwG die deutsche Niederlassung nicht nur als maßgeblich für die Zuständigkeit der Aufsichtsbehörde zu verstehen. Vielmehr sollte die deutsche Niederlassung als Verantwortliche gelten, mutmaßlich zusammen mit der US-amerikanischen Muttergesellschaft als eine einzige Stelle.[101] Das BVerwG vermischte also Fragen der Konturierung der Stelle, und damit des Verantwortlichen, mit solchen der aufsichtsbehördlichen Zuständigkeit. Diese Fragen müssen jedoch auseinandergehalten werden. Zuerst stellt sich die Frage, ob die formelle Zuschreibung der Verantwortlichkeit ausreichend für die Zuständigkeit der Aufsichtsbehörde ist. Zweitens stellt sich die Frage, ob die formelle Zuschreibung der Verantwortlichkeit ausreichend für die Bestimmung der Verantwortlichkeit ist. Drittens stellt sich die Frage, ob eine rechtlich selbstständige Niederlassung mit der Muttergesellschaft als ein Verantwortlicher oder aber als gemeinsam Verantwortliche erachtet werden kann.[102]

Die zweite Frage kann mit einem klaren Nein beantwortet werden. Die formelle Zuschreibung der Verantwortlichkeit ist nicht ausreichend für die Verantwortlichkeit. Maßgeblich sind die tatsächlichen Umstände. Für die DSRL ergab sich dies nur aus der Definition des für die Verarbeitung Verantwortlichen. Für die DSGVO ergibt sich dies zusätzlich aus der Transparenzpflicht in Art. 26 Abs. 2 S. 1 DSGVO und dem Auftragsverarbeiterexzess in Art. 28 Abs. 10 DSGVO. Die Verantwortlichkeit kann für die DSGVO nur durch das Unionsrecht oder das Recht der Mitgliedstaaten formell festgelegt werden. Sonstige Zuschreibungen sind für die Verantwortlichkeit unerheblich.[103] Die Aufklärung der konzerninternen Entscheidungs- und

[101] „ [...] kann hingegen auch eine andere Niederlassung (hier: Deutschland) als Verantwortliche angesehen werden, [...]“ Dazu unten.

[102] Zur Frage der Auftragsverarbeitung durch eine Konzernmutter: Simitis/Hornung/Spiecker/*Petri*, Art. 28 DSGVO, Rn. 24.

[103] Die Unbeachtlichkeit formeller Festlegung ergibt sich implizit aus dem Kriterium der tatsächlichen

Datenverarbeitungsstrukturen ist also für die Ermittlung des Verantwortlichen notwendig.

Die dritte Frage wiederum hängt von dieser Ermittlung ab. Soweit eine Niederlassung mit eigener Rechtspersönlichkeit über die Verarbeitungen in irgendeiner Weise mitentscheidet, ist sie gemeinsame Verantwortliche zusammen mit der Muttergesellschaft. Potenziell ist zwar auch eine Auftragsverarbeitung der Niederlassung gegenüber der Muttergesellschaft denkbar, diese wird aber häufig entweder nicht beabsichtigt oder nachweisbar sein. Sofern die Weisungsgebundenheit als Voraussetzung der Auftragsverarbeitung bei der Niederlassung also nicht besteht, muss diese auch bei minimaler Beteiligung an den Verarbeitungen, mangels einer alternativen Rolle, als gemeinsam Verantwortliche erachtet werden. Eine einheitliche „Konzern-Verantwortlichkeit" lässt sich der DSGVO nicht entnehmen.[104] Der EuGH hat bereits klargestellt das Art. 101 und 102 AEUV nur für die Höhe der Geldbuße zu berücksichtigen ist.[105]

Für die erste Frage zur Zuständigkeit der Aufsichtsbehörde schließlich ist die rein formelle Zuschreibung der Verantwortlichkeit ausreichend. Denn um die tatsächliche Verantwortlichkeit festzustellen, muss die Aufsichtsbehörde möglicherweise erst auf ihre Untersuchungsbefugnisse nach Art. 58 Abs. 1 DSGVO zurückgreifen. Dabei besteht aber auch das Risiko, dass die Aufsichtsbehörde letztlich keine Abhilfebefugnisse ergreifen kann, wenn sie nach Ermittlung der tatsächlichen Verantwortlichkeit nicht federführende Aufsichtsbehörde ist.

Der EuGH übergeht in seinem Urteil zur Vorlage des BVerwG die Problematik der Zuständigkeit der Aufsichtsbehörde komplett, indem er seine Google Spain-Rechtsprechung zur Zuständigkeit der Aufsichtsbehörde[106] auch für solche Sachverhalte für anwendbar erklärt, in denen der Verantwortliche seinen Sitz in der Union hat.[107] In der Rechtssache Google Spain hatte der EuGH es für die Anwendbarkeit der DSRL und Zuständigkeit einer Aufsichtsbehörde ausreichen lassen, dass eine Niederlassung des Verantwortlichen in der Union im Bereich des Werbegeschäftes tätig war. In der Rechtssache Google Spain wurde zwar nur Google Inc. (im Folgenden „Google"), also die amerikanische Muttergesellschaft, als

Entscheidungsmacht, vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 15.

[104] Dazu unten.

[105] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 57.

[106] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 60.

[107] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 64. Dieser Teil der Rechtsprechung dürfte mit dem Prinzip der federführenden Aufsichtsbehörde gem. Art. 56 i.V.m. 60 DSGVO allerdings nicht mehr weiter gelten: ebd., 361 f.

Verantwortliche vom vorlegenden Gericht identifiziert.[108] Man kann die Ausführungen des EuGH aber aufgrund der stets gemeinsamen Nennung von Google Inc. und Google Spain so interpretieren, dass er Google Inc. und Google Spain als gemeinsam Verantwortliche erachtete. Zur Verantwortlichkeit von Facebook Inc. (im Folgenden „Facebook") und Facebook Ireland Ltd. (im Folgenden „Facebook Ireland") äußert sich der EuGH in der Rechtssache Wirtschaftsakademie nur beiläufig:

> *„Es ist festzustellen, dass im vorliegenden Fall in erster Linie die Facebook Inc. und, was die Union betrifft, Facebook Ireland über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheiden, die die auf Facebook unterhaltenen Fanpages besucht haben, und somit unter den Begriff des ‚für die Verarbeitung Verantwortlichen' i.S.v. Art. 2 lit. d RL 95/46 fallen, was in der vorliegenden Rechtssache nicht in Zweifel gezogen wird."*[109]

Unklar bleibt bei dieser Feststellung in welchem Verhältnis Facebook und Facebook Ireland zueinanderstehen. Im weiteren Urteil spricht der EuGH, ohne dies näher zu begründen, davon, dass Facebook zusammen mit Facebook Ireland gemeinsam Verantwortliche seien.[110] Wie sich dies etwa mit dem Wortlaut *„[...] und, was die Union betrifft, Facebook Ireland [...]"* verträgt, wird nicht erläutert.

Die DSGVO selbst setzt sich mit dem Problem der Konturierung der Stelle in Konzernstrukturen, trotz der Definition des Begriffs der Unternehmensgruppe in Art. 4 Nr. 19 DSGVO als

> *„eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht",*

nicht auseinander. Der Begriff der Unternehmensgruppe ist vor allem für die Benennung eines Datenschutzbeauftragten nach Art. 37 DSGVO sowie die verbindlichen internen Datenschutzvorschriften nach Art. 47 DSGVO maßgeblich.[111] ErwGr 48 S. 1 DSGVO deutet zunächst auf eine gemeinsame Verantwortlichkeit von Unternehmen in Konzernen hin. Gemäß diesem Erwägungsgrund können

[108] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 43.
[109] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 30.
[110] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 31, 55, 59 f.
[111] Dazu ErwGr 110 DSGVO.

Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln. Allerdings steht dies mit den Feststellungen aus ErwGr 37 S. 2 DSGVO in einem gewissen Widerspruch, wonach ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, mit diesen zusammen als eine Unternehmensgruppe betrachtet werden sollte. Denn nach diesem Wortlaut hätte nur oder jedenfalls primär das herrschende Unternehmen Entscheidungsmacht und wäre somit per Definition Verantwortlicher. Daneben definiert ErwGr 37 S. 1 DSGVO die Unternehmensgruppe so:

> *„Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann.“*

Denkbar ist also, dass es sich bei ErwGr 37 S. 1 und 2 DSGVO um Alternativen handelt. Wenig hilfreich zum Verständnis der Unternehmensgruppe als einheitliche Stelle oder gemeinsam Verantwortliche ist auch ErwGr 36 S. 8 DSGVO. Demnach soll

> *„die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt.“*

Die grundsätzliche Annahme ist hier offensichtlich, dass das herrschende Unternehmen die Zwecke und Mittel der Verarbeitung festlegt, also wiederum per Definition Verantwortlicher ist.

Zusätzlich verwirrend ist schließlich die Bemessung der Geldbuße gem. ErwGr 150 S. 3 DSGVO anhand des Unternehmensbegriff aus Art. 101 und 102 AEUV.[112] Demnach ist ein funktionaler Unternehmensbegriff anzuwenden. Versteht man nun die an Unternehmensgruppen beteiligten Unternehmen als gemeinsam Verantwortliche, könnte jeweils pro Unternehmen die gesamte Unternehmensgruppe

[112] Dazu: Kapitel 3 C. I. Der funktionale Unternehmensbegriff als Maßstab.

als Maßstab für die Bebußung herangezogen werden. Bereits bei zwei Unternehmen wäre also der doppelte Betrag der durch diese gebildete Unternehmensgruppe maßgeblich.[113] Auflösen läßt sich dieser offensichtlich nicht beabsichtigte Effekt dadurch, dass man ErwGr 150 S. 3 DSGVO dahingehend interpretiert, dass eines der bebußten Unternehmen gesamtschuldnerisch für die Unternehmensgruppe haftet.

Der DSGVO lässt sich systematisch also insgesamt keine klare Konturierung der Stelle für Konzern- bzw. Unternehmensgruppen-Sachverhalte entnehmen.[114] Um dem Wortlaut der Definition des Verantwortlichen, insbesondere hinsichtlich der „juristischen Person", gerecht zu werden, kann aber auch bei einem dominanten Einfluss der Muttergesellschaft oder anderer Konzerngesellschaften auf die fraglichen Verarbeitungen keine eigene Konzern-Verantwortlichkeit gebildet werden. Vielmehr müssen die Unternehmensgesellschaften individuell als solche betrachtet werden. Auch aus Praktikabilitätsgründen scheidet eine einheitliche Konzern-Verantwortlichkeit aus. Denn mangels aufsichtsbehördlicher Befugnisse außerhalb der Union wird eine Aufsichtsbehörde eine solche, abseits von Amtshilfe, kaum nachweisen können, sofern Konzerngesellschaften außerhalb der Union ihren Sitz haben. Daneben kann auch die unzureichende Erfüllung der Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO von nicht in der Union verorteten Konzerngesellschaften kaum effektiv sanktioniert werden. Maßgeblich für die Verantwortlichkeit in Konzernstrukturen ist demnach, welches Unternehmen innerhalb eines Konzerns bzw. einer Unternehmensgruppe über die (Zwecke und Mittel) der Verarbeitung entscheidet und wie viel Entscheidungsautonomie den anderen Unternehmen verbleibt. Da die lokalen Konzerngesellschaften in der Union eigentlich immer in irgendeiner Weise in die Verarbeitungen mit eingebunden sein werden, wird damit regelmäßig eine gemeinsame Verantwortlichkeit zwischen verschiedenen Konzerngesellschaften, etwa Mutter- und Tochtergesellschaft vorliegen. Ausnahmsweise ist auch eine Auftragsverarbeitung bei faktischer Weisungsgebundenheit denkbar. Eine Entscheidung einer nicht-EU-Konzerngesellschaft über die Verarbeitungen vorbei an den lokalen Konzerngesellschaften erscheint hingegen kaum denkbar.

Insgesamt lässt sich keine allgemeine Aussage für eine Verantwortlichkeit innerhalb von Konzernstrukturen allein aufgrund einer generellen wirtschaftlichen Abhängigkeit etwa der Tochtergesellschaften treffen. Die Verantwortlichkeit kann also nicht allein gesellschafts- oder kartellrechtlich bestimmt werden, sondern muss

[113] Entsprechend bei acht Unternehmen der achtfache Betrag.

[114] Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 286 etwa nehmen an, dass Unternehmen im Konzern sich ggü. Dritte seien, aber die Verantwortlichkeit innerhalb des Konzerns delegieren könnten.

datenschutzrechtlich autonom bestimmt werden.[115] Ausgehend von der jeweiligen Entscheidungskompetenz lassen sich die Verantwortlichkeiten in Konzern- bzw. Unternehmensgruppen-Sachverhalten dann weiter bestimmen.[116]

VI. Unternehmen mit Entscheidungsmacht außerhalb der Europäischen Union

Wie bereits angedeutet, stellt sich in Verarbeitungsszenarien, in denen zumindest eines der Unternehmen als Verantwortlicher seinen Sitz[117] außerhalb der Union hat, die Frage, wie eine Niederlassung im Unionsgebiet zu qualifizieren ist. Dies gilt insbesondere für das Szenario, in dem ein Unternehmen mit Sitz außerhalb der Union eine Niederlassung in der Union unterhält, die aber keinerlei Entscheidungsmacht im Hinblick auf die Verarbeitungen hat. Handelt es sich bei dieser Niederlassung um einen von dem Unternehmen separaten Verantwortlichen? Handelt es sich bei der Niederlassung und dem Unternehmen um einen einheitlichen Verantwortlichen oder ist die Niederlassung gar nicht verantwortlich? Weder die EuGH-Urteile in den Rechtssachen Google Spain noch Wirtschaftsakademie geben hierzu eine Orientierung.

Die DSGVO erwähnt zwar grundsätzlich die Hauptniederlassung des Verantwortlichen in Art. 4 Nr. 16 lit. a DSGVO sowie die Niederlassung in ErwGr 22 DSGVO, stellte diese aber nicht in Bezug zum Verantwortlichen. Nach ErwGr 22 DSGVO ist die Rechtsform einer Niederlassung unerheblich. Dies ist nur schwer zu vereinbaren mit der Erwähnung der juristischen Person in der Definition des Verantwortlichen, die sich offensichtlich nur anhand einer Rechtsform konturieren kann. Nach ErwGr 22 DSGVO kann eine Niederlassung also Teil des Verantwortlichen (im Sinne der Stelle) sein, sofern sie keine eigene Rechtspersönlichkeit aufweist. Sie kann gleichzeitig aber auch nicht Teil des Verantwortlichen sein, sofern sie eine Rechtspersönlichkeit besitzt. Ob die Niederlassung Teil des Verantwortlichen oder gemeinsam mit diesem Verantwortlicher ist, bleibt also eine Einzelfallfrage. Hinsichtlich der Urteile des EuGH in den Rechtssachen Google Spain oder Wirtschaftsakademie müssen die jeweiligen Niederlassung nicht als Teil von Google Inc. bzw. Facebook Inc. als Verantwortliche

[115] Vgl. Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 149 f. „the rule "one company, one controller" does not apply".

[116] Vgl. zu Konzernsachverhalten: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 3 f.

[117] Der Sitz des Verantwortlichen ist insoweit erheblich, wie die Aufsichtsbehörde ihre Befugnisse, insbesondere was die Verarbeitung und Geldbußen angeht, sinnvoll nur im Staat des Sitzes des Verantwortlichen durchsetzen kann.

in den USA betrachtet werden, sondern aufgrund ihrer eigenen Rechtspersönlichkeit als mit diesen gemeinsam Verantwortliche.[118]

Da die Niederlassung aber nicht zwangsläufig eine eigene Rechtspersönlichkeit besitzen muss, weist das Konzept der Niederlassung auch nicht zwingend eine Schnittmenge mit dem Verantwortlichen auf. Eine Niederlassung ohne Rechtspersönlichkeit sollte also primär, entsprechend dem Vertreter[119] gem. Art. 27 Abs. 4 DSGVO, als Anlaufstelle für Aufsichtsbehörden und betroffene Personen verstanden werden. Dies ergibt sich im Umkehrschluss auch daraus, dass der Vertreter gem. Art. 3 Abs. 2 DSGVO gerade dann erforderlich ist, wenn keine Niederlassung des Verantwortlichen nach Art. 3 Abs. 1 DSGVO besteht. Der Rechtsgedanke aus Art. 27 Abs. 5 DSGVO findet daher auch für die Niederlassung Anwendung. Nach dieser Norm sind unbeschadet der Benennung eines Vertreters rechtliche Schritte gegen den Verantwortlichen oder Auftragsverarbeiter möglich. Da sich die Konzepte von Niederlassung und Verantwortlichem hinsichtlich der Stelle nicht überschneiden müssen, ist also auch ein Vorgehen gegen eine Niederlassung ohne Rechtspersönlichkeit denkbar. Dies gilt jedenfalls soweit, wie die Verarbeitung im Rahmen der Tätigkeit dieser Niederlassung erfolgt.

Die Maßnahmen gegen den Vertreter und damit auch gegen die Niederlassung sind allerdings ausgehend vom Wortlaut auf Art. 58 Abs. 1 lit. a DSGVO beschränkt. Denn nur dort wird er explizit erwähnt. Es ist aber äußerst fraglich, ob dies Absicht des Unionsgesetzgebers war. Unabhängig von anderen denkbaren Befugnissen der Aufsichtsbehörde ist aber ebenso unklar, inwiefern diese Befugnisse gegen Verantwortliche ohne Sitz in der EU durchgesetzt werden können. So hatte der EuGH in einem Urteil angedeutet, dass Aufsichtsbehörden die Betroffenenrechte ohnehin nicht außerhalb der Union durchsetzen könnten.[120]

Festhalten lassen sich folglich für Verarbeitungsszenarien, in denen ein Unternehmen mit Entscheidungsmacht außerhalb der Union beteiligt ist, folgende Erkenntnisse. Das Unternehmen außerhalb der Union ist aufgrund seiner Entscheidungsmacht stets Verantwortlicher. Soweit eine Niederlassung dieses Unternehmens in der Union mit Rechtspersönlichkeit vorhanden ist, ist diese regelmäßig, soweit sie irgendwie an der Verarbeitung beteiligt ist, zusammen mit dem Unternehmen gemeinsam Verantwortliche. Potenziell kann bei Bestehen einer Weisungsgebundenheit auch eine faktische Auftragsverarbeitung der Niederlassung

[118] So wohl in: EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 31, 55, 59 f.

[119] Siehe zum Vertreter a. ErwGr 80 DSGVO.

[120] EuGH, Urteil vom 24.09.2019 – C-507/17 (Google/CNIL) = GRUR 2019, 1317, Rn. 63 ff.

vorliegen. Soweit die Niederlassung keine eigene Rechtspersönlichkeit aufweist, ist diese entsprechend dem Vertreter gem. Art. 27 Abs. 4 DSGVO als Anlaufstelle für betroffene Personen und Aufsichtsbehörden zu behandeln. Die Niederlassung muss also Anträge der betroffenen Personen sowie Maßnahmen der Aufsichtsbehörden an den Verantwortlichen weitergeben, soweit sie sie nicht selbst erfüllen kann. Da die Niederlassung andererseits aber auch Teil des Unternehmens als Verantwortlichem ist, können gegen die Niederlassung, aber nur in ihrer Funktion als Teil des Verantwortlichen, auch Maßnahmen gegenüber dem Verantwortlichen verhängt werden. Ob diese Maßnahmen über die Niederlassung effektiv durchgesetzt werden können, ist allerdings eine andere Frage. Gibt es schließlich neben dem Unternehmen außerhalb der EU noch eine weitere rechtsfähige Niederlassung in der Union und ist diese ebenso an der Verarbeitung in irgendeiner Weise beteiligt, ist auch diese Niederlassung grundsätzlich gemeinsam Verantwortlicher. Soweit die andere Niederlassung in der Union allerdings keine Rechtspersönlichkeit hat, ist nur die Niederlassung mit Rechtspersönlichkeit in ihrer Position als Verantwortlicher gegenüber den betroffenen Personen und den Aufsichtsbehörden in Anspruch zu nehmen.

VII. Kritik

Wie hier dargestellt, lässt sich das Definitionselement der Stelle nicht komplett losgelöst vom Element der Entscheidung betrachten. Dies gilt für alle Formen der Stelle. Eine Analyse der Stelle kann also nur dann erfolgen, wenn zumindest eine gewisse Entscheidungsautonomie einer bestimmten Stelle festgestellt wurde. Abseits der natürlichen und juristischen Person lässt sich nur dann eine Konturierung der Stelle erzielen, wenn eine organisatorisch abgrenzbare Entscheidungsautonomie festgestellt wurde. Sobald zumindest ungefähr klar ist, wer über die Verarbeitung (mit-)entscheidet, lässt sich diesem eine Organisationseinheit zuordnen, nicht umgekehrt.[121] Ob die (Mit-)Entscheidung über eine Verarbeitung, insbesondere in komplexen Szenarien mit vielen Akteuren aber ohne weiteres erkennbar ist, kann bezweifelt werden. Andererseits bestehen für die Aufsichtsbehörden gerade hier die Untersuchungsbefugnisse aus Art. 58 Abs. 1 DSGVO. Für betroffene Personen sieht die DSGVO eine Unterstützungsfunktion des Auftragsverarbeiters gem. Art. 28 Abs. 3 lit. e DSGVO bzw. des gemeinsam Verantwortlichen gem Art. 26 Abs. 3 DSGVO vor.

[121] Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 20.

Es zeigt sich insgesamt ein doppelter Analyseaufwand bei der Feststellung einer Stelle. Zunächst muss die Entscheidungsautonomie hinsichtlich einer Verarbeitung erkannt werden, dann die zuständige Organisationseinheit für diese Entscheidung geklärt werden. Die Definition des Verantwortlichen ist in dieser Hinsicht zwar sehr flexibel, aber je nach Sachverhalt auch sehr schwierig anzuwenden. Dies ist weniger eine Kritik der Definition als vielmehr die Feststellung, dass die Definition des Verantwortlichen aufgrund ihres hohen Abstraktionsgrades keine Prototypen der Verantwortlichkeit herausgebildet hat. Denkbar wäre insoweit, dass die Aufsichtsbehörden bei bestimmten Voraussetzungen von bestimmten Entscheidungsstrukturen[122] ausgehen könnten und die Verantwortlichen diese Annahmen im Rahmen ihrer Rechenschaftspflicht entkräften müssten.

C. Zweck(e)

> *„Es sei unklar, was denn Zweck überhaupt ist, wie eng oder wie weit der Zweck zu sehen ist, ob Zweck etwa gleich Aufgabe ist oder organisatorisch definiert werden kann usw.“*[123]

Der Zweck[124] als Objekt der Entscheidung des Verantwortlichen wird in der DSGVO nicht weiter definiert.[125] Die Definition des Verantwortlichen und die dazugehörigen Erwägungsgründe verweisen weder explizit noch implizit auf andere Normen, die einen wortgleichen Begriff verwenden. Da es sich bei der DSGVO um sekundäres Unionsrecht handelt, muss der Begriff also entsprechend der unionsrechtlichen Methodenlehre[126] ausgelegt werden. Der grammatikalischen sowie der historischen Auslegung kommen dabei regelmäßig wenig Bedeutung zu. Entscheidend ist vor allem das Telos der Norm sowie die Systematik. Systematisch liegt es nahe, den Zweck aus

[122] So sieht *Keller*, BTLJ[33] (2018), 287, 327 etwa eine Neigung der Aufsichtsbehörden Host-Provider als Verantwortliche zu bewerten.

[123] *Badura*, Anhörungsbeitrag in der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages vom 19. Juni 1989 (Sitzungsniederschrift der öffentlichen Anhörung am 19. Juni 1989, in: Deutscher Bundestag (Hrsg.), Fortentwicklung der Datenverarbeitung und des Datenschutzes: Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 19. und 23. Juni 1989, 1990, 16). Dort ging es allerdings um das BDSG 1990, nicht die DSRL.

[124] Gem. der Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO eigentlich: „die Zwecke“. In der englischen Version: „the purposes“, in der französischen Version: „les finalités“.

[125] *Monreal*, CR 2019, 797, Rn. 26.

[126] Callies/Ruffert/*Wegener*, Art. 19 EUV, Rn. 28 ff.; EuGH, Urteil vom 01.10.2019 – C-673/17 (Planet 49) = EuZW 2019, 916, Rn. 48.

Art. 4 Nr. 7 DSGVO im Zusammenhang mit der Zweckbindung in Art. 5 Abs. 1 lit. b DSGVO zu verstehen.[127] Dies ist auch im Hinblick auf den Telos von Art. 4 Nr. 7 DSGVO schlüssig. Die Zweckfestlegung ist entscheidend für die Verarbeitungsrechtfertigung nach Art. 6 Abs. 1 DSGVO und ist somit Kern der Entscheidung des Verantwortlichen. *Bock* spricht daher bei der Bestimmung der Zwecke von der juristischen Begründbarkeit der Verarbeitung und somit der Rückführung auf eine Rechtsgrundlage.[128] Daneben wird ein Verständnis, das den Zweck aus Art. 4 Nr. 7 DSGVO im Zusammenhang mit der Zweckbindung aus Art. 5 Abs. 1 lit. b DSGVO versteht, auch der einheitlichen Auslegung der verschiedenen Sprachfassungen der DSGVO gerecht.[129]

Die Art. 29-Datenschutzgruppe verstand den Zweck als das „Warum" der Verarbeitung.[130] Der Zweck sei ein „erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet."[131] Die Entscheidung über die Zwecke der Verarbeitung solle allein dem/den (gemeinsam) Verantwortlichen vorbehalten sein.[132] Eine Entscheidung über die Zwecke der Verarbeitung führe also zwingend zu einer Einordnung als Verantwortlicher.[133] Sinnvoller ist es allerdings, den Zweck als das „Wofür" der Verarbeitung zu verstehen. Der Begriff „Wofür" unterstreicht besser die Ziel- bzw. Ergebnisbezogenheit oder genauer die Finalität[134] der Verarbeitung. Zudem steht „Wofür" im Gegensatz zu „Warum" nicht für ein abstraktes Bündel aus Zweck, Motivation und Interesse.[135]

---

[127] So für die DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 16. Für die DSGVO: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 34.

[128] *Bock*, K&R 2019, 30, 31. Insofern ist der Zweck a. essenziell für die Kontrolltätigkeit der Aufsichtsbehörden: *Simitis*, CR 1987, 602, 611.

[129] Sowohl die englische als a. die französische Sprachfassung verwenden identische Begriffe in Art. 4 Nr. 7 DSGVO und Art. 5 Abs. 1 lit. b DSGVO.

[130] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 16; ähnlich a.: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9.

[131] So a.: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 33.

[132] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17 f.

[133] Ebenso: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9.

[134] Vgl. a. den entsprechenden Begriff der französischen Sprachfassung: „la finalité".

[135] Ambivalent („to what end"; or „what for"): *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 35.

Die Ausführungen des EuGH zu den Zwecken der Verarbeitung im Kontext seiner Rechtsprechung zu der (gemeinsamen) Verantwortlichkeit entbehren bislang, insbesondere auch im Hinblick auf ihre Kürze[136], einer systematischen Tiefe, so dass insofern kein besonderer Erkenntnisgewinn vorliegt. Inwiefern der EuGH sich bei gemeinsam Verantwortlichen weg von einem eigentlichen Zweck und hin zu einer Zweckkongruenz oder einem gemeinsamen Interesse bewegt, wird in Kapitel 4 E. I.[137] analysiert.

Eine Behandlung der zahlreichen allgemeinen Probleme rund um die Zweckfestlegung sowie -bindung, abseits des konkreten Bezugs zur Definition des Verantwortlichen, würde an dieser Stelle den Rahmen der Arbeit sprengen. Daher sei an dieser Stelle statt vieler anderer Quellen auf die Dissertationen von *Kring*[138] sowie von *von Grafenstein*[139] verwiesen.

D. Mittel

Ebenso wie zu den Zwecken der Verarbeitung finden sich auch zu den Mitteln der Verarbeitung keine weiteren Erläuterungen in der DSGVO. Zwar verwendet ErwGr 26 S. 3 DSGVO den Begriff Mittel, allerdings geht es dort um die Frage der Personenbeziehbarkeit von Daten. Anhand von Art. 25 Abs. 1 DSGVO wird immerhin deutlich, dass die Mittel der Verarbeitung nicht deckungsgleich mit den technischen und organisatorischen Maßnahmen sind, die der Verantwortliche zu treffen hat. Denn diese Maßnahmen sind zum Zeitpunkt der Festlegung der Mittel zu treffen. Unerheblich ist das Verständnis der einzelnen Elemente der Mittel aber keineswegs. Abhängig davon, welche Elemente der Mittel im Rahmen der Entscheidung erheblich für die Einordnung als Verantwortlicher sind, bestimmt sich in Verarbeitungsszenarien mit mehreren Akteuren auch eine Einordnung als gemeinsam Verantwortliche oder Auftragsverarbeiter.[140]

---

[136] Die Ausführungen in EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, 61 ff. etwa beschränken sich auf drei Randnummern mit insgesamt drei Sätzen.

[137] Kapitel 4 E. I. Das „Interesse“ in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen.

[138] *Kring*, Big Data und der Grundsatz der Zweckbindung im Datenschutzrecht, 2019.

[139] *Grafenstein*, The Principle of Purpose Limitation in Data Protection Laws, 2018.

[140] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 16.

Im ursprünglichen Kommissionsentwurf zur DSRL gab es den Begriff der Mittel noch nicht.[141] Der Verantwortliche bestimmte sich durch die Entscheidung über (neben dem Zweck) die Arten der gespeicherten Daten, mit welchen Vorgängen[142] sie verarbeitet werden sollten und welche Dritte Zugang zu ihnen haben sollten.[143] Der geänderte Kommissionsentwurf behielt diese drei Aspekte, nicht wörtlich, aber inhaltsgleich, bei. Insofern ist der Begriff Mittel in der endgültigen Fassung der DSRL zwar eine Kürzung, aber keine inhaltliche Änderung gegenüber den Entwurfsfassungen.[144]

I. Verständnis der Aufsichtsbehörden[145]

Die Art. 29-Datenschutzgruppe unterteilte die Mittel der Verarbeitung grob in technische und organisatorische Fragen der Verarbeitung sowie die sogenannten wesentlichen Elemente.[146] Insgesamt ginge es bei den Mitteln um das „Wie" der Verarbeitung oder die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird". Die technischen Fragen bzw. Methoden beträfen etwa die verwendete Hard- und Software. Die wesentlichen Elemente[147] der Mittel beträfen unter anderem:

- die zu verarbeitenden Daten[148]
- die Dauer der Verarbeitung
- den Zugang zu den Daten seitens Dritter[149]

---

[141] Siehe zur Genese: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 15 ff.

[142] Gemeint war wohl Verfahren.

[143] BR-Drs. 690/90, 52 f.

[144] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[145] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17 f. und weitgehend identisch a. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9 f.

[146] Vgl. a. die Differenzierung bei: *Bock*, K&R 2019, 30, 31; kritisch zur Differenzierung der Mittel: *Alsenoy*, CLSR[28] (2012), 25, 37.

[147] Vgl. Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 181.

[148] Sinnvollerweise sollte es dabei um eine gröbere Kategorisierung der Daten gehen (etwa: weiße Männer älter als 60 Jahre), nicht die individuelle Auswahl von Datensätzen. Dies deckt sich dann a. mit dem ursprünglichen Kommissionsentwurf und den „Arten personenbezogener Daten": BR-Drs. 690/90, 52 f. Zustimmend wohl: G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40. Daneben kann man darunter a. die Sensibilität der Daten nach Art. 9 und 10 DSGVO verstehen. Das eine Verständnis schließt dabei das andere nicht notwendigerweise aus.

[149] A. dies findet sich im ursprünglichen Kommissionsentwurf: BR-Drs. 690/90, S. 52 f.

- den Zeitpunkt der Löschung der Daten[150]

Ähnlich liest sich die Auflistung des EDPS.[151] Demnach sollen wesentliche Elemente der Mittel die folgenden sein:

- die Art der zu verarbeitenden Daten[152]
- der Zeitraum der Speicherung (der Daten)
- von welchen Personen Daten erhoben werden
- wer Zugriff auf die Daten hat
- wer Empfänger der Daten ist

Die Entscheidung über die technischen und organisatorischen Fragen als Teilaspekt der Mittel sei problemlos an einen Auftragsverarbeiter delegierbar.[153] Hingegen soll die Entscheidung über die eben genannten wesentlichen Elemente der Mittel die Einordnung als Verantwortlicher implizieren.[154] Diese nur bedingte Ausschlagkraft für die Einordnung als Verantwortlicher steht im Gegensatz zur Entscheidung über die Zwecke, die stets eine Einordnung als Verantwortlicher bedinge.[155] Vorschläge zu den wesentlichen Elementen der Mittel durch einen Auftragsverarbeiter sollen nach Ansicht des EDPS möglich sein, solange der Verantwortliche hierüber selbst

[150] Dies kann man a. im Zusammenhang mit der Dauer der Verarbeitung begreifen.

[151] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9 f. Fast identisch: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40. Allerdings wird hier die Frage des Zugangs zu Daten mit der Kategorie von Empfängern verbunden, während der EDPS zwischen beiden trennt.

[152] Hierbei handelt es sich vermutlich um Kategorien von Daten, etwa auch die besonders sensiblen Daten nach Art. 9 und 10 DSGVO.

[153] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17; *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9 f.

[154] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17; *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9 f. scheint nicht nur eine Implikation, sondern direkt eine Einordnung als Verantwortlicher vorzunehmen.

[155] Woher sich dieser Unterschied ergibt, ist nicht ersichtlich. Möglicherweise haderte die Art. 29-Datenschutzgruppe mit dem Wortlaut „Zwecke und Mittel". Widersprüchlich ist diesbezüglich a. die vorläufige Schlussfolgerung in *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18. Ebenso: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 39.

entscheidet.[156] Nach Ansicht des EDPB sind die wesentlichen Mittel eng mit dem Zweck und dem Umfang der Verarbeitung verknüpft und daher grundsätzlich dem Verantwortlichen vorbehalten.[157]

Im Hinblick auf die unwesentlichen Elemente der Mittel, also die technischen und organisatorischen Fragen, weist der EDPB zudem darauf hin, dass die Weisung Maßnahmen nach Art. 32 DSGVO zu treffen, im Vertrag zur Auftragsverarbeitung festgehalten werden sollte.[158] Dabei sollte auch die Unterstützung des Verantwortlichen durch den Auftragsverarbeiter in Bezug auf die Einhaltung der Pflichten der DSGVO festgehalten werden. Im Rahmen der Pflicht des Verantwortlichen technische und organisatorische Maßnahmen nach Art. 24 DSGVO zu ergreifen, sollte der Verantwortliche also vollständig über die Mittel der Verarbeitung durch den Auftragsverarbeiters informiert werden.

Kritisch anzumerken ist im Hinblick auf die unwesentlichen Elemente der Mittel, dass gerade technische Fragen, wie die verwendete Software oder Hardware, durchaus auch die wesentlichen Elemente betreffen können, also etwa welche Daten wie verarbeitet werden.[159] So kann insbesondere bei Standardsoftware gegebenenfalls keine Konfigurationsmöglichkeit des Auftragsverarbeiters hinsichtlich wesentlicher Elemente der Mittel bestehen. Sofern durch die Auswahl der Soft- oder Hardware also auch eine Entscheidung über die wesentlichen Elemente der Mittel erfolgen würde, wäre ein vermeintlicher Auftragsverarbeiter faktisch ein gemeinsam Verantwortlicher.

II. Wesentliche Elemente der Mittel als erforderlicher Vertragsinhalt nach Art. 28 Abs. 3 DSGVO

Die Differenzierung zwischen wesentlichen Elementen und unwesentlichen Elementen der Mittel lässt sich auch aus den Festlegungserfordernissen für eine

[156] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 16 f. Ähnlich wohl: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18.

[157] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40.

[158] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 41 mit Beispiel Call Center.

[159] In diesem Zusammenhang sei an Lawrence Lessig und das Zitat „Code is Law“ erinnert.

Auftragsverarbeitung in Art. 28 Abs. 3 DSGVO ableiten.[160] So muss im Rahmen der Auftragsverarbeitung festgelegt werden:[161]

- Gegenstand
- Dauer
- Art
- Zweck

der Verarbeitung sowie die

- Art der personenbezogenen Daten und die
- Kategorien betroffener Personen

Dabei stellt der Zweck entsprechend der Definition des Verantwortlichen zugegebenermaßen kein Mittel dar. Aus der notwendigen Festlegung durch den Verantwortlichen ergibt sich daher, dass dieser selbst hierüber entscheiden muss. Im Umkehrschluss kann der Auftragsverarbeiter aber auch über die Elemente der Mittel entscheiden, die nicht in Art. 28 Abs. 3 DSGVO als notwendige Festlegung des Verantwortlichen erwähnt werden.

III. Die Mittel in der Rechtsprechung des EuGH

Bezüge zu den wesentlichen Elementen der Mittel finden sich in dem Urteil des EuGH in der Rechtssache Wirtschaftsakademie.[162] So spricht der EuGH davon, dass im Rahmen der Einrichtung bzw. „Parametrierung" der Fanpage (ein individuelles Profil innerhalb einer Plattforminfrastruktur) neben der allgemeinen Beeinflussung der durch den Plattformbetreiber zu erstellenden Besucherstatistik auch die Kategorien der Personen (also der Webseitenbesucher) festgelegt werden, deren Daten hierfür verarbeitet werden sollen.[163]

---

[160] Vgl. Paal/Pauly/*Martini*, Art. 28 DSGVO, Rn. 35 f.; Simitis/Hornung/Spiecker/*Petri*, Art. 28 DSGVO, Rn. 51. Kritisch G/S/S/V/*Kramer*, Art. 28 DSGVO, Rn. 48 f., da Art. 28 Abs. 3 DSGVO nicht explizit den Begriff Mittel erwähnt. Vgl. a. den Gesetzgebungsprozess und die angedachte Voraussetzung der Bedingung: Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 6.

[161] Vgl. a. den notwendigen Inhalt einer Vereinbarung zwischen gemeinsam Verantwortlichen nach EPDS: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 28.

[162] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[163] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36.

In der Rechtssache Fashion ID[164] hatte der Websitebetreiber unter anderem eingewandt, dass er keinen Einfluss auf die an den Plattformbetreiber übermittelten Daten habe. Einräumen lässt sich hier sicherlich, dass der Websitebetreiber die Übermittlung nicht in inhaltlicher Hinsicht beeinflussen konnte.[165] Allerdings scheint es offensichtlich, dass die Entscheidung über das Stattfinden der Übermittlung überhaupt einem, wie auch immer gearteten, Einfluss auf die übermittelten Daten in ihrer Intensität vorgeht.[166] Im Verständnis der Art. 29-Datenschutzgruppe lässt sich insofern argumentieren, dass eine Ermöglichung und damit verbunden auch eine mögliche Beendigung der Verarbeitung, eine Entscheidung über die Dauer der Verarbeitung sowie über den Zugang zu den Daten bedeutet. Gleichermaßen bleibt dies natürlich auf den konkreten Vorgang des Zusammenwirkens beschränkt.

Aus dem Urteil in der Rechtssache NZÖG[167] geht hervor, dass der EuGH hinsichtlich der Mittel etwa die zu verarbeitenden personenbezogenen Daten sowie die einzelnen Parameter einer zu entwickelnden App als maßgeblich erachtet.[168] Konkrete Ausführungen zu dem bei der Verarbeitung angewandten Verfahren finden sich zudem in dem Urteil in der Rechtssache IAB Europe.[169] So betrifft das Verfahren etwa den konkreten technischen Ablauf der verschiedenen Verarbeitungsschritte für einen bestimmten Zweck.

IV. Fazit

Die Differenzierung der Art. 29-Datenschutzgruppe und des EDPB zwischen wesentlichen und unwesentlichen Elementen der Mittel einer Verarbeitung ist sinnvoll und kann zudem aus der Systematik der DSGVO mit den Festlegungserfordernissen in Art. 28 Abs. 3 S. 1 DSGVO begründet werden. Maßgeblich für die Einordnung eines Akteurs anhand einer Entscheidung über die Mittel der Verarbeitung ist vor allem die Entscheidung darüber, welche Arten von personenbezogenen Daten von welchen Kategorien betroffener Personen verarbeitet werden sollen. Dabei ist die Entscheidung über diese Daten nicht auf einer Mikroebene zu treffen, sondern sie kann, wie sich aus dem Wortlaut der Norm ergibt, einen gewissen Abstraktionsgrad aufweisen.

---

[164] Dazu: Kapitel 4 B. III. Fashion ID.

[165] Insofern lag eine „take-it-or-leave-it"-Situation vor.

[166] Vgl. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 10.

[167] Dazu: Kapitel 4 B. IV. NZÖG (Nacionalinis visuomenes sveikatos centras).

[168] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 32.

[169] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 66 f.

E. Entscheidung

Das Definitionselement der Entscheidung ist von elementarer Bedeutung für die Feststellung der Verantwortlichkeit.[170] Dies gilt für singuläre Verantwortliche und erst recht für gemeinsam Verantwortliche.[171] Anhand der eigenen Entscheidung wird der Verantwortliche vom weisungsgebundenen Auftragsverarbeiter abgegrenzt. Rechtshistorisch gesehen ist sie die einzige wesentliche Neuerung im Konzept des Verantwortlichen seit seiner ersten gesetzlichen Fixierung im BDSG 1977.[172] Während das ursprüngliche Übereinkommen Nr. 108 des Europarates[173] noch eine Festlegung der Verantwortlichkeit durch einzelstaatliches Recht vorsah und das BDSG a.F.[174] bis zu seinem Außerkrafttreten 2018 sich, ausgehend vom Wortlaut, rein über die Durchführung der Verarbeitung definierte, legte die DSRL eine Entscheidung über die Verarbeitung als bestimmendes Element des Verantwortlichen zugrunde.[175] Dieses Element der Entscheidung war gerade auch im Hinblick auf die neu eingeführten gemeinsam Verantwortlichen notwendig, um damit überhaupt eine Zuordnung mehrerer Akteure zu einer Verarbeitung zu ermöglichen. Soweit erkennbar fehlt es bislang, knapp 30 Jahre nach Verabschiedung der DSRL, an einer vertieften Auseinandersetzung mit diesem Element der Definition des Verantwortlichen.

Dieses Kapitel analysiert verschiedene Elemente der Entscheidung. Dabei wird zunächst der Frage nachgegangen, ob und falls ja, welche Kenntniselemente eine Entscheidung voraussetzt. Daneben wird erörtert, ob eine Entscheidungsfähigkeit Voraussetzung für eine Entscheidung ist, welche formellen Voraussetzungen eine Entscheidung erfüllen muss und ob die Entscheidung eine technische Kontrolle der Verarbeitung voraussetzt. Schließlich wird die von der Art. 29-Datenschutzgruppe vorgeschlagene Typologie zur Ermittlung einer Entscheidung dargestellt und kritisiert.

Im Hinblick auf die Systematik der DSGVO wird die Entscheidung über Zwecke und Mittel vor allem noch im Rahmen der Definition der Hauptniederlassung in Art. 4 Nr. 16 lit. a DSGVO sowie dem korrespondierenden ErwGr 36 DSGVO erwähnt. So soll nach ErwGr 36 DSGVO für die Hauptniederlassung der Ort ausschlaggebend sein,

---

[170] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 18; Ehmann/Selmayr/*Klabunde/Horvath*, Art. 4 DS-GVO, Rn. 39.

[171] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[172] Dazu: Kapitel 1 B. II. BDSG (1977).

[173] Dazu: Kapitel 1 B. IV. Übereinkommen Nr. 108 des Europarates (1981).

[174] Dazu: Kapitel 1 B. VI. 2. Technischer Ansatz.

[175] Vgl. *Monreal*, PinG 2017, 216, 220.

an dem durch die effektive und tatsächliche Ausübung von Managementtätigkeiten (durch eine feste Einrichtung) Grundsatzentscheidungen zur Festlegung von Zwecken und Mitteln getroffen werden. In Art. 26 Abs. 1 S. 1 DSGVO findet sich die gleiche Definition wie in Art. 4 Nr. 7 DSGVO mit leicht abgewandeltem Wortlaut. Bei gemeinsam Verantwortlichen ist demnach der Akt der Festlegung der Zwecke und Mittel entscheidend. Dass Art. 26 Abs. 1 S. 1 DSGVO aber andere Voraussetzungen als Art. 4 Nr. 7 DSGVO, der ja auch die gemeinsam Verantwortlichen definiert, bedingen wollte, ist nicht ersichtlich.[176]

Rein etymologisch betrachtet bedeutet „entscheiden", dass eine Fragestellung endgültig geklärt, dass in einem Zweifelsfall ein Urteil gefällt oder dass ein Entschluss über eine Auswahl (bestimmend) getroffen wird.[177] Die englische und französische Sprachfassung der DSGVO verwenden das Wort „determine" bzw. „détermine", was im Deutschen mit bestimmen, festlegen oder eben auch entscheiden übersetzt werden kann. Die Bestimmung der Bedeutung von „entscheiden" anhand der Zweckbestimmung des Verantwortlichen als „verantworten" scheint hingegen ein Zirkelschluss zu sein,[178] da die Entscheidung und die sich daraus ergebende Verarbeitung erst die Verantwortung begründet. Das Bezugsobjekt der Entscheidung ist, via deren Zwecke und Mittel, die Verarbeitung und dabei immer der konkrete Vorgang bzw. die Vorgangsreihe.

Der EDPB hält in seinen Leitlinien zum Verantwortlichen fest:

> *„[...] given a particular processing operation, the controller is the actor who has determined why the processing is taking place [...] and how this objective shall be reached [...]. A natural or legal person who* ***exerts such influence*** *over the processing of personal data, thereby participates in the* ***determination*** *of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR."*[179]

In diesem Sinne ist die Entscheidung über die Zwecke und Mittel einer Verarbeitung folglich die Ausübung eines gewissen Einflusses hierüber. Die Frage, was

[176] Dazu: Kapitel 4 C. I. Art. 4 Nr. 7 vs. Art. 26 Abs. 1 S. 1 DSGVO – unterschiedliche Definitionen der gemeinsam Verantwortlichen?

[177] https://www.duden.de/rechtschreibung/entscheiden (abgerufen am 17.07.2024).

[178] Siehe *Monreal*, CR 2019, 797, Rn. 28.

[179] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 35 (Hervorhebung durch den Autor).

Objekt dieses Einflusses ist und wie hoch der Einfluss sein muss, stellt sich vor allem im Rahmen der gemeinsamen Verantwortlichkeit.[180]

I. Vorfrage: Notwendige Kenntniselemente der Entscheidung

Anhand des Wortlauts der Definition des Verantwortlichen lässt sich die Frage, ob die Entscheidung über die Verarbeitung Kenntniselemente aufweist, grundsätzlich schnell beantworten. Liegt eine Verarbeitung vor und wird über deren Zwecke und Mittel entschieden, sind dies die zwingenden, aber zugleich auch ausreichenden Voraussetzungen der Verantwortlichkeit.

Die Frage, ob und wenn ja welche Kenntniselemente für eine Entscheidung über die Zwecke und Mittel einer Verarbeitung nötig sind, ist bislang,[181] soweit ersichtlich, nicht behandelt worden. Hin und wieder ergeben sich aber kurze Randbemerkungen hierzu, so auch in der Rechtssache Google Spain. Google vertrat die Position, es handele sich bei ihr als Suchmaschinenbetreiberin nicht um eine Verantwortliche, da sie weder Kenntnis noch Kontrolle über die Bereitstellung der Suchergebnisse habe.[182] Diese Bereitstellung erfolge vielmehr automatisiert und ohne Unterscheidungsfähigkeit der Suchmaschine zwischen Daten mit oder ohne Personenbezug. Somit läge bereits keine Verarbeitung vor. Der EuGH folgte allerdings dieser Argumentation nicht und stellte eine eigene Verarbeitung[183] sowie eine Verantwortlichkeit der Suchmaschinenbetreiberin fest.[184]

Hinter den Einwänden von Google steckt die Frage, inwiefern eine Automatisierung von Verarbeitungen von einer Verantwortlichkeit befreien kann.[185] Denkbar erscheint, dass dies schon eine Verarbeitung ausschließt oder dass jedenfalls keine Verantwortlichkeit begründet wird. Indessen erscheint der erste Teil der Fragestellung im Hinblick auf die Definition der Verarbeitung in Art. 4 Nr. 2

[180] Dazu: Kapitel 4 H. Die gemeinsame Entscheidung und Kapitel 4 I. Erheblichkeitsschwelle des Entscheidungsbeitrags.

[181] So war etwa die (kurze) Ablehnung subjektiver Elemente bei *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 30 ff. erst nach Abgabe dieser Arbeit berücksichtigungsfähig.

[182] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 22.

[183] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 28.

[184] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 33, 41. Anders noch der Generalanwalt: EuGH, Schlussanträge vom 25.06.2013 – C-131/12 (Google Spain), Rn. 82.

[185] Hierbei handelt es sich um eine Frage, die vor allem im Bereich der Regulierung von Large Language Models (LLMs) virulent werden wird.

DSGVO[186] überflüssig, ist doch Element der Definition: *„[...] mit oder ohne Hilfe **automatisierter** Verfahren ausgeführten Vorgang [...]“*.[187]

1. Kenntnis der Verarbeitung personenbezogener Daten als Voraussetzung einer Verarbeitung?

Ausgangspunkt der Einwände von Google scheint zunächst der Gedanke zu sein, eine Verarbeitung erfordere die Absicht oder jedenfalls die Kenntnis dahingehend, dass personenbezogene Daten verarbeitet werden (also das „ob“).[188] Die Absicht oder Kenntnis könnte dabei auch durch die Fähigkeit eines Programms bzw. einer Maschine, zu unterscheiden, ob ein Personenbezug vorliegt oder nicht, hergestellt werden. Der Wortlaut der Definition der Verarbeitung macht allerdings deutlich, dass es bei der Verarbeitung um einen rein faktischen Prozess[189] geht, in dem personenbezogene Daten verarbeitet werden. So stellt der EuGH im Urteil zu der Rechtssache Google Spain zunächst fest, dass sich unter den von einer Suchmaschine verarbeiteten[190] Daten auch personenbezogene befinden können.[191] Eine Absicht oder Kenntnis des Verantwortlichen hinsichtlich bestimmter Aspekte einer Verarbeitung, wie etwa des Personenbezugs, sei nicht Teil der Definition der Verarbeitung und damit für deren Vorliegen nicht erforderlich.[192] Die von der Suchmaschinenbetreiberin durchgeführten Verarbeitungen fänden sich vielmehr ohne ein solches Erfordernis in der beispielhaften Auflistung der verschiedenen Erscheinungsformen der Definition einer Verarbeitung wieder.[193]

Grundsätzlich erscheint es zwar denkbar, auf die Unterscheidungsfähigkeit eines Programms bzw. einer Maschine hinsichtlich des Personenbezugs abzustellen. Letztlich würde dies aber Folgeprobleme, etwa in der Ermittlung eines Sachverhalts,[194] bedingen

[186] Relevante Diskrepanzen zur Definition der DSRL bestehen nicht.

[187] Vgl. Kühling/Buchner/*Herbst*, Art. 4 Nr. 2 DS-GVO, Rn. 14 zur menschlichen Veranlassung. Vgl. BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 29 zu einem subjektiven Element.

[188] Siehe a.: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 10 Fn. 13.

[189] Die Verwendung von Vorgang wird wegen der Ambiguität hier bewusst vermieden.

[190] Diese Vorgangsreihe beschreibt der EuGH so: „[Tätigkeit,] die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen [...]“ (EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 21).

[191] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 27.

[192] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 28.

[193] So das „auslesen“, „speichern“, „organisieren“, „aufbewahren“, „weitergeben“ und „bereitstellen“, vgl. Art. 2 lit. b DSRL.

[194] Im Hinblick auf den Quellcode und das Urheberrecht sowie Betriebsgeheimnisse.

und potenzielle Umgehungskonstruktionen fördern.[195] Unklar wäre zudem, wo diese Unterscheidungsfähigkeit hinsichtlich des Personenbezugs als Voraussetzung zu verorten wäre. Bereits die Verarbeitung pauschal abzulehnen, ist jedenfalls, abseits einer kontextspezifischen Regelung, etwa von Large Language Models (LLMs), im Interesse eines umfassenden Schutzes der betroffenen Personen nicht sinnvoll.[196] Folglich ist die Kenntnis eines Personenbezugs für eine Verarbeitung nicht erforderlich.

2. Objekte der Entscheidung

Neben der mangelnden Unterscheidungsfähigkeit der Suchmaschine hinsichtlich des Personenbezugs verwies Google auch darauf, dass sie selbst keine Kenntnis und Kontrolle über die personenbezogenen Daten im Rahmen der Verarbeitung der Suchmaschine habe und daher nicht Verantwortliche für diese Verarbeitung sein könne.[197] Parallel zur Frage, ob die Verarbeitung also eine Absicht oder Kenntnis hinsichtlich des Personenbezugs voraussetzt, stellt sich diese Frage auch für den Verantwortlichen bei der Entscheidung über die Verarbeitung.

Die Definition des Verantwortlichen verlangt eine Entscheidung über die Zwecke und Mittel der Verarbeitung personenbezogener Daten. Rein grammatikalisch sind die Objekte der Entscheidung also die Zwecke und Mittel der Verarbeitung.[198] Anhand der konkreten Verarbeitung bemisst sich, worüber der Verantwortliche entscheiden,[199] also „Kontrolle“[200] haben muss.

[195] Bspw. im Rahmen einer Programmierung, die Personenbezug einfach nicht beachtet.

[196] Vgl. die Erwägungen in EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 30, 34.

[197] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 22.

[198] Missverständlich die Art. 29-Datenschutzgruppe: „diese Verarbeitung ist letztendlich das Objekt der „gemeinsamen Kontrolle““ in: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[199] Vgl. EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 33.

[200] Die Art. 29-Datenschutzgruppe setzt In WP 169 die Entscheidung über die Verarbeitung mit der Kontrolle gleich, vgl. etwa *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

Zwar spricht die Definition des Verantwortlichen von einer Entscheidung über die Zwecke und Mittel der Verarbeitung personenbezogener Daten, allerdings enthält schon die Definition der Verarbeitung in Art. 4 Nr. 2 DSGVO selbst das Satzfragment „personenbezogene[n] Daten". Gleiches gilt für den auf die Verarbeitung bezugnehmenden sachlichen Anwendungsbereich der DSGVO in Art. 2 Abs. 1 DSGVO. Inhaltlich findet sich also hinsichtlich des Personenbezugs von Daten kein „mehr" in der Definition des Verantwortlichen gegenüber der Definition der Verarbeitung. Eine notwendige Absicht oder Kenntnis hinsichtlich des Personenbezugs einer Verarbeitung ist weder anhand der Definition der Verarbeitung noch des Verantwortlichen ersichtlich. Der Verantwortliche entscheidet über die Zwecke und Mittel der Verarbeitung – einschließlich der verwendeten personenbezogenen Daten –, nicht aber über die personenbezogenen Daten als solche. Auch die Zwecke und Mittel der Verarbeitung beinhalten den Aspekt des Personenbezugs nicht notwendigerweise. Denkbar ist etwa das Szenario, dass ein Verantwortlicher vermeintlich anonymisierte Daten für eine Studie verarbeitet, sich darunter allerdings auch nicht anonymisierte Daten befinden. Auch in diesem Szenario wird über Zwecke und Mittel der Verarbeitung entschieden, ohne dass überhaupt ein Bewusstsein des Personenbezugs seitens des Verantwortlichen besteht. Folglich ist weder eine Absicht noch eine abstrakte oder konkrete Kenntnis des Verantwortlichen dahingehend erforderlich, dass eine Verarbeitung auch personenbezogene Daten betrifft. Ausreichend ist vielmehr die faktische Verarbeitung von personenbezogenen Daten, sowohl für die Verarbeitung als auch für die Verantwortlichkeit.[201] Mit anderen Worten: Die Verarbeitung muss personenbezogene Daten beinhalten, der Verantwortliche entscheidet aber nur über die Zwecke und Mittel der Verarbeitung. Der Personenbezug ist Voraussetzung der Verarbeitung, nicht aber der Entscheidung. Selbst im Falle der fehlenden faktischen Kenntnis einer Verarbeitung personenbezogener Daten liegt eine Kontrolle des Verantwortlichen wenigstens insoweit vor, dass er die Verarbeitung wieder beenden kann. Die Entscheidung zur Verarbeitung begründet die Verantwortung für eben diese.[202] Dies bedeutet etwa für gemeinsam Verantwortliche, dass keine tatsächliche Kenntnis der konkreten gemeinsamen Verarbeitung vorliegen muss. Eine jedenfalls einseitige Antizipation unkonkretisierter Verarbeitungen reicht aus.[203] In den Leitlinien zum

[201] *Sartor* hält in seiner Analyse der Google Spain-Entscheidung dagegen und argumentiert, dass teleologisch betrachtet eine so weitgehende Verantwortlichkeit des Suchmaschinenbetreibers und vergleichbarer Intermediäre nicht beabsichtigt sein kann: *Sartor*, MJ[21] (2014), 564, 567 ff.

[202] *Monreal*, CR 2019, 797, Rn. 27.

[203] So etwa die Bereitstellung des Social Plugins durch den Plattformanbieter in: EuGH, Urteil vom

Verantwortlichen weist der EDPB explizit darauf hin, dass jeder, der Daten verarbeite, sich vergewissern sollte, ob diese auch personenbezogene Daten beinhalten und welche Pflichten der DSGVO daraus erwachsen.[204] Ein Akteur werde auch dann als Verantwortlicher behandelt, wenn er nicht bewusst personenbezogene Daten verarbeite oder davon ausgeht, dies nicht zu tun.

Soweit ersichtlich gibt es bislang eine gerichtliche Entscheidung, die dieser Argumentation widerspricht. In dieser Entscheidung hatte das höchste italienische Gericht (Corte di Cassazione) in einem Fall, der Youtube betraf, die Privilegierungen der e-Commerce-RL[205] auf die DSRL bzw. deren italienische Umsetzung angewandt.[206] Dadurch wurde eine Verantwortlichkeit erst ab Kenntnis des Inhalts eines Videos begründet.[207] Diese Entscheidung wurde allerdings nicht weiter aufgegriffen. Sie dürfte auch mit dem neuen Wortlaut der Privilegierungen in Art. 4 ff. DSA, der von „haften" spricht nicht weiter vereinbar sein.

3. Rechtsprechung des EuGH

Der EuGH beschränkt sich im Urteil zu der Rechtssache Google Spain darauf zu betonen, dass die Suchmaschinenbetreiberin über Zwecke und Mittel der Verarbeitung entscheide.[208] Dabei sei unerheblich, dass die auf den Websites von Dritten veröffentlichten personenbezogenen Daten nicht der Kontrolle der Suchmaschinenbetreiberin unterliegen. Denn diese vorgelagerte Verarbeitung sei auch nicht Anknüpfungspunkt der Verantwortlichkeit, sondern die der Tätigkeit der Suchmaschine, des „Webcrawlens" der Webseiten.[209] Eine Ausnahme von der Verantwortlichkeit aufgrund mangelnder Kontrolle über die vorgelagerte Verarbeitung auf den Websites sei wegen des weiten Verständnisses des Begriffs des Verantwortlichen ausgeschlossen, damit ein umfassender Schutz der betroffenen Personen gewährleistet werden kann.[210]

29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977. Vgl. a. *Monreal*, CR 2019, 797, Rn. 40, der keine explizite Einigung zwischen gemeinsam Verantwortlichen, wohl aber einen Beitrag zur Verarbeitung verlangt.

[204] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 44.

[205] Mittlerweile in dem DSA enthalten.

[206] Corte di Cassazione, Cass. sez. tre Penale, 3 febbraio 2014, n. 5107/14 (It.).

[207] Mit ausführlicher Diskussion: *Keller*, BTLJ[33] (2018), 287, 358 ff.

[208] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 32 ff.

[209] Vgl. EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 28. Inwiefern sich diese Verarbeitung von der vorgelagerten Verarbeitung auf den jeweiligen Webseiten unterscheidet, erläutert der EuGH in: ebd., Rn. 35 ff.

[210] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 34.

Im Urteil zu der Rechtssache Fashion ID[211] hingegen erwähnt der EuGH die Kenntnis bzw. das Wissen des Verantwortlichen im Zusammenhang mit der Einbindung des Social Plugins durch den Websitebetreiber in seine Website. Dabei hält der EuGH im Rahmen seiner Ausführungen zu den Mitteln der Verarbeitung fest, dass der Websitebetreiber das Social Plugin offenbar in dem Wissen eingebunden habe, dass dieses als Werkzeug zum Erheben und zur Übermittlung von personenbezogenen Daten der Besucher dieser Seite diene.[212] Daneben habe er mit der Einbindung des Social Plugins entscheidend die Erhebung und Übermittlung der Daten beeinflusst.[213] Insgesamt hält der EuGH fest, dass der Websitebetreiber somit über die Mittel, die der Erhebung und Übermittlung zugrunde lagen, entschieden habe.[214] Bedauerlicherweise macht der EuGH hier keine weiteren Ausführungen zum „Wissen" des Verantwortlichen.

4. Herleitung aus der Systematik

Sofern man sich der Frage notwendiger Kenntniselemente[215] positiv nähert, also fragt, welche Kenntniselemente für eine Entscheidung vorhanden sein müssen, stellt sich zunächst die grundlegende Frage, ob das Definitionselement der Entscheidung weniger eine bewusste Entscheidung über die Verarbeitung, als vielmehr eine Entscheidung über die tatsächlichen Konsequenzen eines Handelns bedeutet.[216]

a) Kenntnis der Zwecke?

Die Frage der Erforderlichkeit einer Kenntnis stellt sich bei den Zwecken der Verarbeitung insgesamt nicht, da eine Festlegung der Zwecke notwendigerweise deren Kenntnis voraussetzt. Aufgrund des Zweckbindungsgrundsatzes in Art. 5 Abs. 1 lit. b DSGVO, der auch die Zweckfestlegung beinhaltet, ist die Kenntnis der Zwecke in systematischer Hinsicht also zwingend. Der Zweck einer Verarbeitung wird zudem auch bei fehlender Kenntnis des Personenbezugs von Daten festgelegt.

---

[211] Dazu: Kapitel 4 B. III. Fashion ID.
[212] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77.
[213] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 78.
[214] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 79.
[215] Als Minus zur Absicht.
[216] Vgl. zur Notwendigkeit eines „Verarbeitungswillens": Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 61, 67.

b) Kenntnis der Mittel?

Neben den Zwecken muss aber auch über die Mittel der Verarbeitung entschieden werden. Für die Mittel gibt es anders als beim Zweck keinen systematischen Zwang zu deren Festlegung oder Kenntnis. Sofern eine Kenntnis der Mittel insgesamt nicht notwendig sein sollte, stellt sich die Frage, ob es Konsequenzen hat, und wenn ja welche, wenn der Verantwortliche keine oder unzureichende Kenntnis über die Mittel hat.

Klar ist zunächst, dass zumindest eine faktische Entscheidung über die Mittel der Verarbeitung vorliegen muss, da ohne diese Entscheidung keine Verarbeitung stattfinden kann. Dies gilt insbesondere dann, wenn man zwischen wesentlichen[217] und unwesentlichen Elementen der Mittel differenziert. Eine Verarbeitung, bei der nicht klar ist, welche Daten verarbeitet werden, kann allein logisch nicht stattfinden. Denkbar ist auch eine Entscheidung durch „Unterlassen", etwa, wenn der Verantwortliche die Entscheidung über die wesentlichen Elemente der Mittel einer Software oder Hardware überlässt. Aber auch in diesem Fall lässt sich in der Entscheidung zur Verwendung bestimmter Software bzw. Hardware eine bewusste Entscheidung erkennen. Selbst im Falle einer Auftragsverarbeitung muss der Verantwortliche zumindest über die Vorschläge eines Auftragsverarbeiters hinsichtlich der wesentlichen Elemente der Mittel entscheiden, will der Auftragsverarbeiter nicht Gefahr laufen, selbst Verantwortlicher zu werden.[218] Folglich lässt sich die Entscheidung des Verantwortlichen über die Mittel zusammenfassend so verstehen, dass sich aus dem Verhalten des Verantwortlichen zumindest die Voraussetzungen für die Durchführung der Verarbeitung überhaupt ableiten.

Bewusste Entscheidungen über bestimmte Elemente der Mittel erscheinen damit als eine Art Obliegenheit des Verantwortlichen. Befasst sich der Verantwortliche nicht bewusst mit diesen Elementen, riskiert er damit beispielweise eine Ausweitung der Verantwortlichkeit hinsichtlich der verarbeiteten Daten oder erfolgenden Verarbeitungen. Ebenso sind Verstöße oder erweiterte Pflichten im Hinblick auf Art. 24, 25 und 32 DSGVO denkbar. Diese Verstöße oder Pflichten ergeben sich dabei aber aus dem Ausmaß der Verarbeitung, mit dem sich der Verantwortliche nicht näher befasst hat. Plastisch bedeutet die fehlende Entscheidung über die wesentlichen Elemente der Mittel für die zu verarbeitenden Daten etwa, dass sie folglich

[217] Dazu: Kapitel 2 D. Mittel.

[218] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 116; *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 16 f.

uneingeschränkt alle verfügbaren Daten betrifft. Für die Verarbeitungsdauer bedeutet sie gegebenenfalls eine unbegrenzte Dauer. Dies gilt jedenfalls dann, wenn diese Elemente nicht durch die Methode der Verarbeitung oder die verwendete Soft- oder Hardware bedingt sind. Über die Entscheidung zu der verwendeten Methode, Soft- oder Hardware ist deren Mittelfestlegung wiederum dem Verantwortlichen zuzurechnen.

Entscheidet ein Verantwortlicher also nicht bewusst über die Mittel der Verarbeitung, verhindert dies nicht seine Verantwortlichkeit, sondern hat Konsequenzen auf deren Rechtsfolgenseite. Dies gilt für das Ausmaß seiner Verantwortlichkeit, für aufsichtsbehördliche Maßnahmen und die Haftung gegenüber betroffenen Personen. Ist es einem Verantwortlichen etwa nicht möglich, Datenübermittlungen von Soft- oder Hardware zu erkennen, entbindet ihn das nicht von seiner Verantwortlichkeit, sondern wird auf der Rechtsfolgenseite berücksichtigt. Würde man in dieser Situation bereits keine Verantwortlichkeit annehmen, wäre die Wahrnehmung der Betroffenenrechte nicht möglich. Auch die Anordnung einer Einstellung der Verarbeitung durch die Aufsichtsbehörde wäre nicht möglich. Es bliebe aus datenschutzrechtlicher Perspektive rein bei der Eigeninitiative eines Nicht-Verantwortlichen.

Daneben hat die fehlende bewusste Entscheidung über die Mittel auch rein praktische Konsequenzen für die Wahrnehmung der Pflichten durch den Verantwortlichen. So kann es an der Erkenntnis fehlen, dass eine Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO vorliegt oder eine Datenschutzfolgeabschätzung nach Art. 35 DSGVO notwendig ist.

Hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten und hierfür gegebenenfalls erforderlicher Absichtselemente des Verantwortlichen liegt auch zumindest ein Urteil des VG Mainz vor.[219] In der konkreten Entscheidung ging es um die Videoüberwachung des Grundstücks eines Einkaufszentrums und in Teilen auch dessen Umfeldes. Dabei befasste sich das VG mit der Frage, ob aufgrund der Videoüberwachung und der damit verbundenen Möglichkeit der Erfassung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO, etwa ethnische Herkunft oder Gesundheitsdaten,[220] auch die damit verbundenen zusätzlichen Anforderungen an die Verarbeitungsrechtfertigung einschlägig seien.[221] Das VG Mainz kam zu dem Schluss, dass die Erfassung solcher besonderen Kategorien personenbezogener Daten

[219] VG Mainz, Urteil vom 24.09.2020 – 1 K 584/19.MZ.
[220] Dazu: VG Mainz, Urteil vom 24.09.2020 – 1 K 584/19.MZ, Rn. 28.
[221] VG Mainz, Urteil vom 24.09.2020 – 1 K 584/19.MZ, Rn. 27 ff.

im Rahmen der Videoüberwachung zwar generell möglich sei. Sie wäre aber nicht Absicht des Betreibers der Videoüberwachung, so dass er diesbezüglich auch keine Auswertungsabsicht habe.[222] Der Betreiber beabsichtige vielmehr durch die Videoüberwachung Strafprävention und -verfolgung. Er habe aber keine Absicht hinsichtlich der Verwertung der besonders sensiblen Daten.

Diese Argumentation scheint allerdings allein schon deswegen zu kurz gegriffen, weil gerade besonders sensible Daten, wie die ethnische Herkunft oder etwa Gesundheitsdaten wie eine Brille oder ein Rollstuhl, zur Identifizierung eines potenziellen Täters dienlich sein können. Daneben scheint es zielführender, die Auswertungsabsicht nicht als eigenes Kriterium zu konstruieren, sondern, abseits einer besonderen Festlegung der Art der zu verarbeitenden Daten (also der Kategorien) im Rahmen der Mittel,[223] die Notwendigkeit der Erhebung im Zusammenhang mit den Zwecken der Verarbeitung zu analysieren.[224] Sofern der Zweck der Verarbeitung nicht erkennbar die Erfassung besonderer Kategorien von Daten betrifft, sondern dies vielmehr inzident erfolgt, scheint eine Anwendung von Art. 9 DSGVO tatsächlich nicht angebracht. Sinnvoll erscheint insofern eine teleologische Reduktion von Art. 9 DSGVO dahingehend, dass aus den Zwecken entweder eine Absicht erkennbar ist oder jedenfalls eine offensichtliche Notwendigkeit besteht, solche Daten zu verwenden. Alternativ wäre de lege ferenda eine Unterscheidung zwischen einer intendierten Verarbeitung und einer nicht intendierten Verarbeitung von Daten nach Art. 9 DSGVO zu ergänzen.[225]

Hinsichtlich der Kenntnis der Mittel lässt sich abschließend festhalten, dass diese nicht konkret erforderlich ist. Der Verantwortliche muss allerdings die Mittel der Verarbeitung, insbesondere wie sie sich aus Art. 28 Abs. 3 S. 1 DSGVO ergeben, zumindest mittelbar durch indirekte Auswahl oder Delegation festgelegt haben, so dass es überhaupt zu einer faktischen Verarbeitung kommt.

---

[222] VG Mainz, Urteil vom 24.09.2020 – 1 K 584/19.MZ, Rn. 28 f. Zur Auswertungsabsicht als Kriterium: Gola/Heckmann/*Schulz*, Art. 9 DSGVO, Rn. 13.

[223] Dazu: Kapitel 2 D. Mittel.

[224] So wohl a.: *European Data Protection Board*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, 29.01.2020, Rn. 63 ff. Zur Entscheidung des VG Mainz *Grages*, https://www.cr-online.de/blog/2020/11/09/verarbeitung-besonderer-datenkategorien-erhoehte-anforderungen-nur-bei-auswertungsabsicht/ (abgerufen am 17.07.2024).

[225] Vergleichbar etwa zur Differenzierung einer Verarbeitung mit intendiertem Personenbezug und nicht intendiertem Personenbezug bei: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 68 ff.

c) Notwendige Kenntniselemente und Kennenmüssen bei gemeinsam Verantwortlichen

Bei gemeinsam Verantwortlichen stellt sich, jedenfalls auf der Rechtsfolgenseite, die Frage, inwiefern Kenntniselemente zugerechnet werden können oder ein Kennenmüssen ausreicht. Diesbezüglich ist der Sachverhalt aus der Rechtssache Google Spain nicht mit dem aus Fashion ID vergleichbar. So musste sich der Verantwortliche in der Rechtssache Google Spain als singulärer Verantwortlicher notwendigerweise alle Details der Verarbeitung im Rahmen seiner Entscheidung zurechnen lassen. In der Rechtssache Fashion ID hingegen konnten Elemente der Entscheidung über die Zwecke und Mittel der Verarbeitung verschiedenen Akteuren zugerechnet werden.

Bei gemeinsam Verantwortlichen ist die Kenntniszurechnung insgesamt nicht trivial, da die eigene Entscheidung eines gemeinsam Verantwortlichen ihn, als notwendige Bedingung der gemeinsamen Verantwortlichkeit, auch gegenüber dem Auftragsverarbeiter oder dem Verantwortlichen untergeordneten Personen[226] abgrenzt.[227] Dies gilt auch dahingehend, dass gemeinsam Verantwortliche nicht eine eigene Rechtsfigur bilden, sondern individuell Verantwortliche mit einer gewissen Verbundenheit darstellen.[228] Folglich ist mangels der Möglichkeit einer unmittelbaren Kenntniszurechnung eine Analyse notwendig, welche Kenntniselemente in der individuellen Entscheidung eines gemeinsam Verantwortlichen über Zwecke und Mittel der Verarbeitung vorliegen müssen. Hat ein potenziell gemeinsam Verantwortlicher keine hinreichende Kenntnis und liegt auch kein Fall eines Kennenmüssens[229] vor, könnte dessen Verantwortlichkeit schlicht abgelehnt werden. Denn im Falle einer Ablehnung dieser Verantwortlichkeit kann die Verantwortlichkeit immer noch den anderen gemeinsam Verantwortlichen bzw. einem singulären Verantwortlichen zugerechnet werden. Das Problem einer unverantworteten Verarbeitung[230] bestünde in diesem Fall nicht. Folglich bietet die gemeinsame Verantwortlichkeit teleologisch betrachtet gegenüber dem singulären Verantwortlichen auch die Möglichkeit weitere Voraussetzungen oder umgekehrt Ausschlusskriterien zu berücksichtigen.

Hanloser entnimmt dem Urteil des EuGH in der Rechtssache Fashion ID,[231] dass der potenziell gemeinsam Verantwortliche sich der eigenen Ermöglichungshandlung,

[226] I.S.v. Art. 29 DSGVO.
[227] Vgl. unten: Kapitel 2 G. IV. Das Eigeninteresse als eigener Zweck?
[228] Dazu: Kapitel 4 C. IV. Gemeinsam Verantwortliche als Rechtssubjekt sui generis?
[229] Dazu unten.
[230] Hierzu: Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 121.
[231] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77.

der ermöglichten Verarbeitung in ihrer konkreten Form sowie dem kausalen Ermöglichungszusammenhang bewusst sein muss.[232] Ein Kennenkönnen oder -müssen sei nicht ausreichend. Dies scheint allerdings eine Überdehnung der Feststellungen des EuGH zu sein. Grundsätzlich setzt der Begriff der Entscheidung oder Festlegung[233] zunächst nur voraus, dass eine minimale Kenntnis über Zwecke und Mittel besteht.[234] So kann etwa aus dem Zweck, dessen Kenntnis seiner Festlegung inhärent ist, auf ein Kennenmüssen der Mittel geschlossen werden.[235] Abseits eines solchen Schlusses vom Zweck auf die Mittel, stellt sich aber die Frage, inwiefern Kenntniselemente hinsichtlich der Mittel vorhanden sein müssen oder im Rahmen eines Kennenmüssen zugerechnet werden können. Diese Kenntniselemente müssen jedenfalls beinhalten, dass überhaupt Datenflüsse stattfinden und/oder Akteure außer den durch die Weisungsgebundenheit Privilegierten i.S.v. Art. 29 DSGVO Zugriff auf die Daten haben. Daher sind für die Frage der Kenntnis insgesamt die wesentlichen Elemente der Mittel einzubeziehen.[236] So verlangt auch der EDPS, dass jeder der gemeinsam Verantwortlichen vor einer Verarbeitung jedenfalls Kenntnis vom allgemeinen Zweck und den wesentlichen Elementen der Mittel der Verarbeitung besitzt.[237]

Während das Problem des erforderlichen Grades der Kenntnis der Mittel in der Rechtssache Fashion ID noch zu vernachlässigen war, da der Einbau des Programmcodes des Social Plugins in die eigene Website zumindest grundlegende Kenntnis des Webdesigns und der damit verbundenen Datenflüsse voraussetzt, sind andere Szenarien denkbar, in denen nicht zwangsläufig ein solch technisches Verständnis potenziell gemeinsam Verantwortlicher angenommen werden kann. Dann stellt sich die Frage, inwiefern ein Kennenmüssen der Mittel ausreichend wäre.

So ist etwa das Szenario denkbar, dass ein Unternehmen eine Software auf den Rechnern seiner Arbeitnehmer einsetzt, die personenbezogene Daten von diesen Arbeitnehmern erhebt und an den Softwareanbieter übermittelt. Ist dieses Feature dem Unternehmen gar nicht bekannt, da es selbst eine oberflächliche Prüfung der Software

---

[232] *Hanloser*, ZD 2019, 455, 459. A. Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 10 sprach in der 2. Aufl. noch von einer bewussten Entscheidung im Rahmen der gemeinsam Verantwortlichen.

[233] Gem. Art. 26 Abs. 1 DSGVO.

[234] Vgl. dazu *Brühann*, DuD[28] (2004), 201, 206 in Bezug auf die Rechtssache Lindqvist (EuGH, Urteil vom 06.11.2003 – C-101/01 (Lindqvist) = EuGRZ 2003, 714-722). In diesem Fall ging es allerdings nicht um eine gemeinsame Verantwortlichkeit.

[235] Vgl. *Brühann*, DuD[28] (2004), 201, 206 zur Absicht von Frau Lindqvist die Daten einer unbestimmten Zahl von Dritten zur Kenntnis zu geben.

[236] Dazu: Kapitel 2 D. Mittel. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[237] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 23.

versäumt hat, verstößt es bereits gegen äußerst geringe technische Sorgfaltspflichten.[238] In diesem Fall überzeugt es nicht, eine gemeinsame Verantwortlichkeit mit dem Softwareanbieter deshalb abzulehnen, weil das Unternehmen keine Kenntnis über die Verarbeitung hat. Andererseits scheint die Möglichkeit der Kenntnis der Erhebung von Daten im Rahmen staatlicher Überwachungsmaßnahmen, etwa durch die Ausnutzung von Softwarelücken im Rahmen von Online-Durchsuchungen, Quellen-TKÜ oder allgemein Staatstrojanern kaum mehr einem Unternehmen, das eine solch belastete Software einsetzt, im Rahmen der Voraussetzungen einer gemeinsamen Verantwortlichkeit zuzumuten.[239] Hier muss auch zwischen einer Verantwortlichkeit und einer Verletzung des Schutzes personenbezogener Daten i.S.v. Art. 4 Nr. 12 DSGVO, Art. 33 DSGVO abgrenzt werden.

Daher muss für die Kenntnis der Mittel bei potenziell gemeinsam Verantwortlichen ein gewisser Sorgfaltsmaßstab gelten.[240] Dieser Sorgfaltsmaßstab ist im Zusammenhang mit einer Prüfungspflicht von Soft- oder Hardware zu verstehen.[241] Eine Prüfungspflicht der verwendeten Technik ergibt sich auch als Obliegenheit aus der Risikoabschätzung nach Art. 25 DSGVO sowie der potenziell nach Art. 35 DSGVO notwendigen Datenschutz-Folgeabschätzung.[242] Diese Prüfungspflicht ist vergleichbar mit der Verpflichtung des Verantwortlichen aus Art. 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern zusammenzuarbeiten, die hinreichende Garantien dafür bieten, dass die Verarbeitung im Einklang mit der DSGVO erfolgt.[243]

Da die Entscheidung über die Mittel, insbesondere die Auswahl der zu verarbeitenden Daten und das Verfahren mit dem sie verarbeitet werden, eng mit der Entscheidung über die Zwecke zusammenhängt, ist zu prüfen, ob das fragliche Element der Mittel der Funktionsweise der verwendeten Technik entspricht. Entspricht das fragliche Element nicht der Funktionsweise der Technik oder widerspricht es dieser sogar, kann kein Kennenmüssen vermutet werden. Dies ergibt sich allein daraus, dass in diesem Fall nicht über den Zweck, den dieses Element erfüllt, entschieden wurde. Eine Haftung im Zusammenhang mit Art. 25 und 32 DSGVO wird dadurch allerdings nicht ausgeschlossen.

---

[238] Vgl. Szenarien sind auch im Rahmen von SDKs, APIs u.ä. denkbar.

[239] Vgl. das Beispiel von SDKs bei *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 250 f.; *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 71 f. hingegen lässt allein das faktische Handeln ausreichen.

[240] Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 135 ff.

[241] So wohl a.: Simitis/Hornung/Spiecker/*Hansen*, Art. 25 DSGVO, Rn. 21.

[242] Sydow/Marsch/*Mantz*, Art. 25 DSGVO, Rn. 21 f. m.w.N.

[243] Siehe dazu: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 18.

Die Sorgfaltspflicht wäre jedenfalls dann verletzt, wenn das Äquivalent einer grob fahrlässigen Unkenntnis im Rahmen der Entscheidung über die Mittel vorliegt.[244] Im Rahmen der Sorgfaltspflicht des Verantwortlichen ist ein Kennenmüssen folglich immer bei dokumentierten, offen erkennbaren Eigenschaften einer Technik anzunehmen. Wird dieser Sorgfaltsmaßstab verletzt, erfolgt auch bei faktischer Unkenntnis der Mittel eine Zurechnung im Rahmen eines Kennenmüssen.

Hinsichtlich des Sorgfaltsmaßstabs schließt sich die Frage an, ob im Rahmen der Unkenntnis ein allgemeiner, ein gruppenbasierter[245] oder ein individualisierter Maßstab gilt. Da dem Datenschutzrecht explizite Bezüge zum Zivil- oder Strafrecht und den damit verbundenen Verschuldens- sowie Vorsatzkonzepten fehlen,[246] ist ein individualisierter oder gruppenbasierter Maßstab nicht angebracht. Dies gilt allein schon aus Bestimmtheitsgründen. Beim Element der Kenntnis oder des Kennenmüssen innerhalb der Entscheidung handelt es sich vielmehr um einen datenschutzrechtlich autonomen Begriff. Die DSGVO unterscheidet zudem nicht zwischen verschiedenen Typen von Verantwortlichen, etwa Unternehmen, Vereinen, Parteien etc.[247] Ausnahmen, Privilegierungen und Ähnliches für bestimmte Verarbeitungskontexte bestimmen grundsätzlich Art. 2 Abs. 2 DSGVO sowie Art. 85 ff. DSGVO. Dementsprechend gibt es keine globalen Privilegierungen oder Auflagen für bestimmte Verantwortliche in der DSGVO, sondern immer nur Lockerungen spezifisch zu konkreten Verpflichtungen.[248] Auch hieran würde ein Sorgfaltsmaßstab, der an die Definition des Verantwortlichen selbst anknüpft, scheitern. Vernünftig lässt sich ein Sorgfaltsmaßstab für das Kennenmüssen daher, abseits einer gesetzlichen Regelung, vor allem durch richterliche Rechtsfortbildung festlegen. Dabei dürfte es sich dann vermutlich, im Rahmen der bisherigen Einzelfallrechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit, um einen individualisierten Maßstab handeln. Aus wissenschaftlicher Perspektive wäre ein Sorgfaltsmaßstab der an die Vorgaben zur Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO sowie zu technisch und organisatorischen Maßnahmen gem. Art. 24 f., 32 DSGVO anknüpft wünschenswert. Hier scheint es naheliegend hinsichtlich des Sorgfaltsmaßstabes auf das Risiko der Verarbeitung abzustellen. Dies kann aber zugebenermaßen nur dann gelten, wenn sich

[244] Anders *Hanloser*, ZD 2019, 455, 459, der positives Wissen voraussetzt.

[245] Etwa im Hinblick auf die Sachkunde.

[246] Vgl. Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 25. Ein Verschuldensmaßstab findet sich nur vereinzelt, etwa im Kontext von Geldbußen, vgl. EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 61 ff.

[247] Vgl. die Erwägungen zu einer Privilegierung von Verbänden und Vereinen im Gesetzgebungsverfahren zur DSRL in BT-Drs. 12/8329, S. 6, 16.

[248] BT-Drs. 12/8329, S.16: „ [...] eine Globalbefreiung ist hingegen nicht erforderlich [...]“ (zur DSRL).

der Verantwortliche wenigstens teilweise einer Verarbeitung personenbezogener Daten bewusst ist. Daneben scheinen Anlehnung an einen allgemeinen zivilrechtlichen Haftungsmaßstab denkbar.

II. Vorfrage: Entscheidungsfähigkeit

Neben der Frage der notwendigen Kenntniselemente für eine Entscheidung stellt sich zudem die Frage, ob eine Entscheidungsfähigkeit für die Entscheidung erforderlich ist, und falls dem so ist, wann sie vorliegt.[249] Die folgenden Erwägungen gelten dabei, trotz des Anknüpfens an Kinder, entsprechend auch für Erwachsene unter rechtlicher Betreuung.[250] Die DSGVO thematisiert, prominent in Art. 8 DSGVO, Kinder nur als betroffene Personen, nicht aber als Verantwortliche.[251] Ausgehend von der Definition des Verantwortlichen wäre auch ein Kind grundsätzlich Verantwortlicher. Dies gilt erst recht dann, wenn man bei singulären Verantwortlichen von einem rein faktischen[252] Entscheidungsbegriff ausgeht.[253] Bei singulären Verantwortlichen lässt sich das Ausmaß der Verarbeitung aufgrund der dem Kind zur Verfügung stehenden Mittel[254] aber regelmäßig im Rahmen der elterlichen Aufsicht bzw. bei Erwachsenen der rechtlichen Betreuung begrenzen. Diese Vermutung gilt hingegen nicht für Szenarien, in denen potenziell gemeinsam Verantwortliche vorliegen. Zu denken wäre hier etwa an die Verarbeitung personenbezogener Daten im Kontext von Social Media. Eine solche Verarbeitung dürfte der kindlichen Fähigkeit zur Nachvollziehbarkeit schnell entgleiten.

Anknüpfend an die Ausführungen zu den notwendigen Kenntniselementen bei gemeinsam Verantwortlichen muss ein Kind also zum einen das Verhältnis zwischen seinem Handeln und einem damit verbundenen Zweck erfassen können, als auch ein grobes Verständnis der wesentlichen Elemente der Mittel besitzen. Dies bedeutet zudem, dass sich ein Kind des Kausalzusammenhangs zwischen seinem Handeln und einer Verarbeitung überhaupt, auch in Form einer Zugangsermöglichung zu Daten, bewusst sein können muss. Eine tatsächliche Unkenntnis im konkreten Falle ist zwar unschädlich, allerdings muss zumindest eine abstrakte Kenntnis möglich sein. Je nach Komplexität der technischen Gegebenheiten ist ein unterschiedlicher Maßstab anzulegen, so dass abseits einer gesetzlichen Festlegung einer Entscheidungsfähigkeit

[249] Vgl. *Golland*, ZD 2020, 397, 399.
[250] Dabei würden die rechtlichen Betreuer an die Stelle der Eltern treten.
[251] *Kienle*, PinG 2020, 208, 213.
[252] Also nur an die Konsequenzen einer Verarbeitung für die Entscheidung hierüber anknüpft.
[253] So etwa: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 27 f.
[254] Handschriftliche Aufzeichnungen, Smartphone-Aufnahmen, digitale Notizen u.ä.

keine Vermutung für eine solch abstrakte Kenntnis besteht. Zudem sind im Hinblick auf die Entscheidungsfähigkeit eines Kindes auch die Aufsichts- und Aufklärungspflichten der Eltern zu beachten.[255] Insgesamt ist ein Maßstab vergleichbar zur Deliktsfähigkeit nach § 828 BGB naheliegend. Die Altersschwelle des Art. 8 Abs. 1 DSGVO zur Einwilligung lässt sich für die Verantwortlichkeit nicht übertragen, da ein Eingriff in die Grundrechtssphäre des Kindes sich grundsätzlich von einem Eingriff des Kindes in fremde Grundrechtssphären unterscheidet.

Kommt man zum Schluss, dass ein Kind, auch unter Beachtung der elterlichen Aufklärungspflichten, nicht imstande war die Konsequenzen seines Handelns, im Sinne einer Entscheidung, zu überblicken, ist der Begriff des Verantwortlichen teleologisch zu reduzieren und das Kind als nicht verantwortlich anzusehen.[256] Ist das Kind grundsätzlich nicht entscheidungsfähig, liegt auch eine Verantwortlichkeit oder Haftung der Eltern fern.[257] Denn diese haben keine Entscheidung über die Verarbeitung getroffen. Daneben besteht auch keine Ersatzverantwortlichkeit oder -haftung der Eltern im Rahmen der DSGVO, vergleichbar zu § 832 BGB. Insofern kommt es dann, jedenfalls abseits anderer gemeinsam Verantwortlicher, zu einer unverantworteten Verarbeitung. Für den Fall, dass das Kind grundsätzlich entscheidungsfähig ist, gleichzeitig aber eine Verletzung der elterlichen Aufsichts- und Aufklärungspflichten vorliegt, sollte eine gemeinsame Verantwortlichkeit des Kindes und der Eltern im Hinblick auf die Pflichten und Haftung nach der DSGVO angenommen werden. Allerdings wäre hier der Abschluss einer Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO im Wege einer teleologischen Reduktion entbehrlich.

III. Rechtmäßigkeit und Form der Entscheidung

Die Befugnis eine Entscheidung über eine Verarbeitung zu treffen, mit anderen Worten, die Rechtmäßigkeit der Entscheidung als solche, wirkt sich nicht auf die Bestimmung der Verantwortlichkeit aus.[258] Insbesondere spielt es keine Rolle, ob der Verantwortliche zur Entscheidung rechtlich befugt ist oder ob der Verantwortliche formell benannt wurde. Zum einen ergibt sich dies aus dem Wortlaut der Definition, da die Entscheidung dort nicht weiter als rechtmäßig qualifiziert wird. Zum anderen ergäbe dies auch nach dem Telos der Norm keinen Sinn. So ist es gerade bei einer

[255] Vgl. *Kienle*, PinG 2020, 208, 214.

[256] Ähnlich wohl *Kienle*, PinG 2020, 208, 213, aber mit Fokus auf ein Unvermögen hinsichtlich der Erfüllung der Verpflichtungen.

[257] *Kienle*, PinG 2020, 208, 214.

[258] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11 f.

unrechtmäßigen Verarbeitung wichtig, dass betroffene Personen ihre Rechte wahrnehmen und Aufsichtsbehörden Maßnahmen ergreifen können.

Die Entscheidung über die Verarbeitung unterliegt zudem keinem besonderen Formerfordernis. Im Rahmen der Rechtssache Jehovan todistajat[259] hatte der EuGH festgehalten, dass insbesondere die Schriftform nicht erforderlich sei, da die Definition des Verantwortlichen hierfür keinerlei Anhaltspunkte gäbe.[260] In der Rechtssache NZÖG hatte der EuGH weitere Ausführungen zu formellen Kriterien gemacht. So sei unerheblich, ob ein Verantwortlicher in der Datenschutzerklärung genannt werde, sofern er der Nennung nicht ausdrücklich oder stillschweigend zugestimmt habe.[261] Unerheblich sei auch, ob ein Vertrag zwischen einem Verantwortlichen und einem an der Verarbeitung beteiligten Dritten bestehe, ob ein Verantwortlicher eine Anwendung, die die Verarbeitungen durchführt, erwerbe oder ob ein Verantwortlicher der Veröffentlichung einer Anwendung durch einen beteiligten Dritten zugestimmt habe.[262] Bei gemeinsam Verantwortlichen sei zudem eine förmliche Vereinbarung über die Zwecke und Mittel der Verarbeitung nicht erforderlich.[263] Schließlich sei auch die für gemeinsam Verantwortliche bestehende Pflicht zum Abschluss einer Vereinbarung gem. Art. 26 Abs. 1 S. 2 DSGVO nicht konstitutiv für die gemeinsame Verantwortlichkeit, sondern, wie sich aus dem Wortlaut ergebe, Folge dieser.[264] Festhalten lässt sich also, dass bislang keine formellen Kriterien für die Entscheidung über die Zwecke und Mittel einer Verarbeitung ersichtlich sind.

IV. Entscheidung als technische Kontrolle der Verarbeitung?

In der Rechtssache Fashion ID[265] ist erkennbar, dass der Vorlage des OLG Düsseldorf ein sehr technikorientiertes[266] Verständnis der Verantwortlichkeit zugrunde lag.[267] So lautete Vorlagefrage 2: „Ist [...] der Einbindende ‚für die Verarbeitung Verantwortlicher' [...], wenn er selber diesen Datenverarbeitungsvorgang nicht

[259] Dazu: Kapitel 4 B. II. Jehovan todistajat.
[260] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 67.
[261] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 34.
[262] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 35.
[263] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 44
[264] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 45; *Dovas*, ZD 2016, 512, 514; *Mester*, DuD 2019, 167. Unverständlich daher: *Brüggemann*, CR 2018, 581, 581.
[265] Dazu: Kapitel 4 B. III. Fashion ID.
[266] Dazu: Kapitel 1 B. VI. 2. Technischer Ansatz. Kritisch a.: *Monreal*, CR 2019, 797, Rn. 36.
[267] Exemplarisch *Hacker*, MMR 2018, 779, 780: „Maßgeblich muss vielmehr die konkrete Mitgestaltung der (Mittel oder Zwecke der) Datenverarbeitung selbst sein, die bei Fanpages durch die Auswahl der Parameter (Einstellung der Kriterien und Aufgreifkategorien der Verarbeitung) für Facebook Insight erfolgt."

beeinflussen kann?“[268] Dass ein solch technisches Mikromanagement der Verarbeitung nach dem maßgeblichen unionsrechtlichen Verständnis nicht notwendig ist, ergibt sich allerdings aus zwei Faktoren.

Zum einen können etwa im Rahmen der Auftragsverarbeitung insbesondere technische und organisatorische Fragen an den Auftragsverarbeiter delegiert werden,[269] soweit diese nicht der Festlegung durch den Verantwortlichen nach Art. 28 Abs. 3 DSGVO unterliegen. Mit anderen Worten: Der Verantwortliche muss nur über die wesentlichen Elemente der Mittel der Verarbeitung gegenüber dem Auftragsverarbeiter entscheiden.[270]

Zum anderen muss der Verantwortliche aber auch keinen Zugang zu den verarbeiteten Daten haben. Dies ergibt sich bereits aus der Definition des Verantwortlichen. Ausreichend ist eine Entscheidung über die Mittel und somit auch über die verarbeiteten Daten.[271] In der Rechtssache NZÖG etwa hielt der EuGH fest, dass sich eine Verantwortlichkeit nicht nur aus der eigenen Verarbeitung von personenbezogenen Daten ergebe, sondern auch wenn personenbezogene Daten im eigenen Namen (eines Verantwortlichen) verarbeitet würden.[272] In dem späteren Urteil in der Rechtssache État Belge betonte der EuGH unter Verweis auf die Rechtssache Google Spain[273] erneut, dass die von einem Verantwortlichen weiterverarbeiteten personenbezogenen Daten nicht seiner Kontrolle unterliegen müssten.[274] Dass auch ein Zugang zu den verarbeiteten Daten entbehrlich ist, hat der EuGH wiederum in dem Urteil in der Rechtssache Jehovan todistajat[275], jedenfalls für gemeinsam Verantwortliche, bestätigt.[276] Orientiert man sich allerdings streng am Wortlaut des Urteils („[...] setzt die gemeinsame Verantwortlichkeit [...] nicht voraus, dass jeder von ihnen Zugang zu den betreffenden personenbezogenen Daten hat.“), dürfte aber zumindest für einen der gemeinsam Verantwortlichen der Zugang zu den Daten notwendig sein. Rückschlüsse aus dem Konzept des Auftragsverarbeiters nach Art. 28

[268] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 37, 42.

[269] Vgl. für die DSRL: *Monreal*, PinG 2017, 216, 219.

[270] Vgl. für die DSRL: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 31.

[271] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 45. Unklar: Simitis/*Dammann*, § 3 BDSG a.F., Rn. 225. Dieser scheint die Verantwortlichkeit dort enden zu lassen, wo die Sachherrschaft über die Daten vollkommen aufgegeben wird.

[272] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 36.

[273] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 34.

[274] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265, Rn. 38.

[275] Dazu: Kapitel 4 B.II. Jehovan todistajat.

[276] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 69.

DSGVO auf das Verhältnis der gemeinsam Verantwortlichen untereinander dürften hingegen nicht zielführend sein. Denn der gemeinsam Verantwortliche hat, anders als der Auftraggeber, kein Weisungsrecht gegenüber den anderen gemeinsam Verantwortlichen. Somit kann er abseits vertraglicher Regelung die verarbeiteten Daten nicht an sich ziehen. Der EDPB erwähnt als Beispiel für den nicht erforderlichen Zugang zu verarbeiteten Daten ein Marktforschungsunternehmen in der Rolle eines Auftragsverarbeiters, das dem Auftraggeber anonymisierte Statistiken über seine Kunden übermittelt.[277] Zumindest nach Ansicht der Aufsichtsbehörden wäre also auch bei einer Auftragsverarbeitung kein Zugang des Verantwortlichen zu den Daten notwendig.[278]

Insgesamt muss der Verantwortliche zwar die für die Verarbeitung erforderlichen grundsätzlichen Festlegungen[279] treffen und sie verantworten.[280] Er muss im Zweifel aber keinen eigenhändigen Durchgriff auf die Verarbeitung als solche oder die Daten haben.[281] Es reicht, wenn er dies durch Weisung, also Entscheidung, erreichen kann.[282] Allein deswegen war der Wortlaut des BDSG a.F., wonach eine „[v]erantwortliche Stelle [...] jede Person oder Stelle [sei], die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“[283], irreführend, da eine irgendwie geartete Delegation der Durchführung der Verarbeitung so nur im Bereich der Auftragsverarbeitung möglich war. Eine eigenhändige, singuläre Verantwortlichkeit implizierte notwendigerweise die Möglichkeit des eigenhändigen Zugriffs auf die Verarbeitung. Entscheidung und direkter Zugriff auf die Verarbeitung waren also nach dem Wortlaut des BDSG a.F. notwendigerweise miteinander verbunden, mindestens durch eine Weisung gegenüber dem Auftragsverarbeiter. Eine Trennung von Entscheidung über und Zugriff auf die Verarbeitung war mangels der Umsetzung des Konzeptes der gemeinsam Verantwortlichen gar nicht denkbar.

---

[277] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 45 Beispiel Marktforschung. Dabei ist für die Abgrenzung zwischen Auftragsverarbeitung und separatem Verantwortlichen erheblich, wie detailliert die Weisungen ggü. dem Marktforschungsinstitut sind.

[278] Unklar auch, da die referenzierte EuGH-Entscheidung nur gemeinsam Verantwortliche betraf: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 10.

[279] Eben Zwecke und wesentliche Elemente der Mittel.

[280] Vgl. a. das Konzept der rechtlichen und praktischen Kontrolle bei: *Alsenoy*, CLSR[28] (2012), 25, 33. Ebenso Simitis/*Dammann*, § 3 BDSG a.F., Rn. 224 zur Verantwortung für den Datenumgang und für die Verarbeitungsmedien, die etwa bei der Auftragsverarbeitung auseinanderfallen sollen.

[281] Verwundert: *Lezzi/Oberlin*, ZD 2018, 398, 400. Ähnlich: *Jung/Hansch*, ZD 2019, 143, 144.

[282] Vgl. zu gemeinsam Verantwortlichen: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 41.

[283] § 3 Abs. 7 BDSG a.F.

Maßgeblich für die Entscheidung über Zwecke und Mittel der Verarbeitung ist aber – auch wenn es tautologisch klingen mag – nur die Entscheidung.[284] Der Verantwortliche muss nicht jede Einzelheit der Verarbeitung direkt beeinflussen können, er muss sie aber sehr wohl wenigstens indirekt kontrollieren können.[285]

V. Typologie anstatt formeller Analyse (Art. 29-Datenschutzgruppe / Europäischer Datenschutzausschuss)

Aufgrund der Vielzahl denkbarer Verarbeitungsszenarien schlug die Art. 29-Datenschutzgruppe vor, den Verantwortlichen – als funktionelles Konzept[286] – anhand einer faktischen Analyse und nicht anhand einer formellen Analyse zu bestimmen.[287] Ausschlaggebend für eine Analyse sollte also der tatsächliche Einfluss eines Verantwortlichen sein, nicht formelle Kriterien. Dementsprechend wollte die Art. 29-Datenschutzgruppe im Rahmen einer Typologie[288] aus rechtlichen und/oder faktischen Umständen auf einen tatsächlichen Einfluss (auf die Verarbeitung) schließen, der wiederum einer Entscheidung entsprechen sollte. Der EDPB, als Nachfolgergremium der Art. 29-Datenschutzgruppe, spricht diesbezüglich von einem Einfluss auf die Verarbeitung anhand der Ausübung von Entscheidungsmacht.[289] Ebenso sollen aber auch Umstände einbezogen werden, die gegen einen solchen tatsächlichen Einfluss sprechen. Im Rahmen der Typologie bildete die Art. 29-Datenschutzgruppe drei Kategorien:

- Verantwortung aufgrund einer ausdrücklichen rechtlichen Zuständigkeit
- Verantwortung aufgrund einer implizierten Zuständigkeit
- Verantwortung aufgrund eines tatsächlichen Einflusses

[284] Vgl. a. *Monreal*, CR 2019, 797, Rn. 33.

[285] Vgl. a. Ehmann/Selmayr/*Klabunde/Horvath*, Art. 4 DS-GVO, Rn. 39: der Verantwortliche muss über die Entscheidung hinaus nicht an der Durchführung der Verarbeitung beteiligt sein.

[286] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 12.

[287] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12. Der Begriff formelle Analyse scheint hier ungünstig gewählt. Vielmehr soll eine Analyse anhand formeller Kriterien vermieden werden.

[288] Dies soll anhand von Faustregeln und praktischen Annahmen erfolgen.

[289] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 20.

1. Verantwortung aufgrund einer ausdrücklichen rechtlichen Zuständigkeit

Die Kategorie der ausdrücklichen rechtlichen Zuständigkeit sollte nach Ansicht der Art. 29-Datenschutzgruppe zum einen den zweiten Teil der Definition des Verantwortlichen umfassen. Demnach kann, sofern Zwecke und Mittel der maßgeblichen Verarbeitung durch Unionsrecht oder das Recht des Mitgliedstaats vorgeben sind, der Verantwortliche bzw. die Kriterien seiner Benennung nach Unionsrecht oder dem Recht des Mitgliedstaats vorgesehen werden.[290] Zum anderen sollten damit auch Rechtsvorschriften erfasst seien, die bestimmten Rechtssubjekten die Aufgabe oder die Verpflichtung auferlegen, Daten zu verarbeiten.[291] Die Aufgabenzuweisung müsse in diesem Fall notwendigerweise eine Datenverarbeitung bedingen. Durch die Aufgabenzuweisung oder Verpflichtung zur Datenverarbeitung ergebe sich dann entsprechend die Verantwortlichkeit. Diese Kategorie zeichnet sich also durch einen direkten (Verpflichtung) oder jedenfalls offensichtlichen (Aufgabe) Kontext einer Datenverarbeitung aus. Inwiefern zwischen einer expliziten Benennung des Verantwortlichen bzw. den Kriterien seiner Benennung und einer impliziten Benennung durch Aufgabenzuweisung und/oder Verpflichtung zur Datenverarbeitung unterschieden werden sollte, erscheint fraglich. Dies zeigt sich nicht zuletzt dadurch, dass die Art. 29-Datenschutzgruppe beide Fälle in einer Kategorie zusammenfasst.

2. Verantwortung aufgrund einer implizierten Zuständigkeit

Die Verantwortung aufgrund einer implizierten Zuständigkeit liege dann vor, wenn sie sich aus allgemeinen gesetzlichen Bestimmungen oder geltender Rechtspraxis in bestimmten Rechtsgebieten ergebe.[292] Für die Bestimmung der Verantwortlichkeit in dieser Kategorie seien die bestehenden traditionellen Rollen richtungsweisend, die üblicherweise eine bestimmte Verantwortlichkeit implizieren würden. Basierend auf der funktionellen Rolle solcher Stellen solle damit einhergehend auch die

[290] Dazu: Kapitel 2 F. Benennung durch (materielles) Gesetz.

[291] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12 f. Die Art. 29-Datenschutzgruppe verwendet dafür das Beispiel einer Sozialversicherung, die für die Durchführung ihrer Aufgaben ein Register führt. Vgl. hierzu a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 24.

[292] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 13. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 27.

Entscheidungsmacht[293] über die Verarbeitungen bestehen. Im Gegensatz zur ausdrücklichen rechtlichen Zuständigkeit liege hier also kein offensichtlicher Kontext einer Datenverarbeitung vor, allerdings bedinge eine funktionelle Rolle abseits der Datenverarbeitung auch eine Entscheidungsmacht über diese. Beispiele für eine solche implizierte Zuständigkeit seien Arbeitgeber in Bezug auf die Daten ihrer Arbeitnehmer, Verleger in Bezug auf Daten ihrer Abonnenten oder Verbände in Bezug auf Daten ihrer Mitglieder oder Mitwirkenden. Die implizierte Zuständigkeit erfasse allerdings auch Behörden mit bestimmten Verwaltungsaufgaben, die keine ausdrücklichen Regelungen zum Datenschutz aufweisen. Als konkretes Beispiel für diesen funktionellen Ansatz erwähnt die Art. 29-Datenschutzgruppe ErwGr 47 DSRL.[294] Dieser stellt die Vermutung auf, dass der Absender einer Nachricht für die Verarbeitung der Inhaltsdaten verantwortlich ist, der Telekommunikationsanbieter hingegen nur für die zusätzlichen Betriebs-, also insbesondere die Verkehrs- und Rechnungsdaten.[295] Ein weiteres Beispiel für die funktionelle Rolle eines Verantwortlichen sieht der EDPB in der Tätigkeit einer Anwaltskanzlei.[296] Zwar gäbe es keine spezifische Zuweisung der Verantwortlichkeit im Rahmen der Tätigkeit einer Anwaltskanzlei, auch nicht in der Mandatierung, allerdings entspreche die Verantwortlichkeit der notwendigen Datenverarbeitung aufgrund der Tätigkeit einer Anwaltskanzlei.

In seinen Leitlinien zum Verantwortlichen gibt der EDPB die Kategorie der implizierten Zuständigkeit auf und ordnet sie der Verantwortung aufgrund eines tatsächlichen Einflusses zu.[297]

---

[293] *Kremer*, CR 2019, 225, Rn. 11 verwendet den Begriff der Verfügungsgewalt über die Verarbeitung. Dieser scheint aber aufgrund der dinglichen Assoziationen eher unangebracht.

[294] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 13 f. Beispiel 1 (Telekommunikationsbetreiber); ähnlich mit Bezug zu ErwGr 47 DSRL: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 27 Beispiel Telekommunikationsbetreiber.

[295] Vertiefend: *Brühann*, DuD[28] (2004), 201, 205. Aufgrund der rechtlichen Natur von ErwGr (Callies/Ruffert/*Wegener*, Art. 19 EUV, Rn. 32) dürfte dies unabhängig vom Inhalt nur eine implizierte Zuständigkeit klarstellen.

[296] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 27.

[297] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 27.

3. Verantwortung aufgrund eines tatsächlichen Einflusses

Falls sich die Verantwortlichkeit aufgrund einer Analyse der Fakten ergebe, ordnete die Art. 29-Datenschutzgruppe dies der Kategorie der Verantwortung aufgrund eines tatsächlichen Einflusses zu.[298] Diese Kategorie sei insbesondere im Fall von rechtswidrigen Verarbeitungen wichtig. Beispielhaft hierfür seien Verarbeitungsszenarien, die teilweise dem Willen der beteiligten Akteure widersprächen, etwa bei dem Auftragsverarbeiterexzess.[299] Bei der Verantwortung aufgrund eines tatsächlichen Einflusses sollten alle relevanten Fakten einbezogen werden, um einen bestimmenden[300] Einfluss auf die Verarbeitung nachweisen zu können.[301] Dabei sei nicht die Art oder Natur der Stelle ausschlaggebend für ihre Einordnung als Verantwortliche, sondern ihre konkreten Aktivitäten in einem spezifischen Kontext.[302] Daher könne sich die Einordnung eines Akteurs auch je nach Verarbeitungsvorgang oder Vorgangsreihe ändern.

Soweit vorhanden schlug die Art. 29-Datenschutzgruppe eine Analyse der vertraglichen Beziehungen der an einer Verarbeitung potenziell beteiligten Parteien[303] vor.[304] Aufgrund einer Analyse der vertraglichen Beziehungen könnten die Verantwortlichkeit dann einer oder mehreren beteiligten Parteien zugeordnet werden. Dabei könnte sich die Verantwortlichkeit entweder direkt aus dem Vertrag ergeben oder aber durch die Vertragsgestaltung indiziert sein, etwa wenn eine der Vertragsparteien eine vorherrschende Stellung im Hinblick auf die Verarbeitung einnimmt. Trotz der Indizwirkung sollten die vertraglichen Festlegungen allerdings auf ihre Plausibilität hin überprüft werden. Es bestehe also kein zwangsläufiger Schluss von den vertraglichen Festlegungen auf die Verantwortlichkeit. Dies sei gerade im Hinblick

[298] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 14 f.

[299] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess; vgl. dazu a. das SWIFT-Beispiel unten.

[300] Die Leitlinien zum Verantwortlichen sprechen hier von einem „determinative influence". Dies kann man mit entscheidendem Einfluss übersetzen. Allerdings wäre dies dann quasi-tautologisch, da sich die Entscheidungsmacht über eine Verarbeitung aus dem entscheidenden Einfluss auf diese ergäbe.

[301] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 25.

[302] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 26.

[303] Die beteiligten Parteien stellen scheinbar die im Kontext einer Verarbeitung identifizierbaren Akteure dar.

[304] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 14; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 28 f.

auf die Vertragsfreiheit der Parteien zu beachten. So könnte eine Verantwortlichkeit auch entgegen einer expliziten vertraglichen Festlegung bestehen. Ebenso könnte auch die vertragliche Einordnung einer Stelle, etwa als Auftragsverarbeiter, den Tatsachen widersprechen.[305] Die Bedeutung der Analyse der Verantwortung aufgrund eines tatsächlichen Einflusses werde insbesondere dort deutlich, wo eine Partei sich über die vertraglichen Festlegungen hinwegsetze, so etwa im Fall von SWIFT.[306] Hier wurde das Unternehmen vom US-Finanzministerium per Verwaltungsakt dazu aufgefordert, personenbezogene Daten, die ursprünglich im Auftrag von Finanzinstituten für kommerzielle Zwecke verarbeitet worden waren, auch für Zwecke der Bekämpfung der Finanzierung terroristischer Aktivitäten an das US-Finanzministerium herauszugeben. Indem es dieser Aufforderung durch eigene Entscheidung nachkam, wurde es damit ungeachtet der vertraglichen Festlegung zum Verantwortlichen. Unabhängig von potenziell vorhandenen vertraglichen Beziehungen sollten also die tatsächlichen Umstände maßgeblich seien, gerade wenn diese vertraglichen Festlegungen den tatsächlichen Umständen widersprächen.

Neben den potenziell vorhandenen Vertragsbedingungen sollte der Grad der tatsächlich ausgeübten Kontrolle, der den betroffenen Personen vermittelte Eindruck sowie die berechtigten Erwartungen der betroffenen Personen aufgrund dieser Außenwirkung[307] zur Analyse der Verantwortlichkeit herangezogen werden.

Dabei stellt sich aber die berechtigte Frage, ob sich eine Verantwortlichkeit nur anhand des Eindrucks bzw. der Erwartungen der betroffenen Personen tatsächlich begründen lässt.[308] Als Ansatzpunkt für eine weitere Analyse mag dieser Eindruck bzw. die Erwartungen förderlich sein, zur tatsächlichen Begründung aber nicht hinreichend.[309] Ansonsten käme es zu einer Anscheinsverantwortlichkeit, die nicht notwendigerweise mit der tatsächlichen Verantwortlichkeit übereinstimmen würde. Wie in diesem Fall die Betroffenenrechte, ohne Zugriff auf die Daten oder auch nur eine Verbundenheit mit dem/den tatsächlich Verantwortlichen, bearbeitet werden könnten, ist völlig unklar. Ein tatsächlicher Einfluss auf die Verarbeitung durch solche Anscheinsverantwortlichen bestünde ja gerade nicht notwendigerweise. Auch

[305] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 29.

[306] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[307] Es wird nicht klar, was genau hiermit gemeint ist. Vermutlich sind es die Erwartungen, die aus dem Eindruck der betroffenen Personen erwachsen.

[308] Zustimmend scheinbar: *Monreal*, CR 2019, 797, Rn. 36.

[309] Ähnlich: Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 149; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 113, 197 ff.

aufsichtsbehördliche Maßnahmen gegenüber Anscheinsverantwortlichen könnten maximal im Rahmen von Unterlassungsanordnungen oder Sanktionen bestehen. Sicherlich ist eine gewisse Handhabe der Aufsichtsbehörden gegenüber solchen Akteuren zwecks Transparenz für die betroffenen Personen wünschenswert. Allerdings scheint die Annahme einer vollwertigen Verantwortlichkeit im Rahmen einer solchen Anscheinsverantwortlichkeit zu weit. Sinnvoll erscheint die Annahme einer solchen Anscheinsverantwortlichkeit vielmehr dann, wenn eine Einwirkungsmöglichkeit des Anscheinsverantwortlichen auf den tatsächlichen Verantwortlichen besteht.

4. Fazit der Art. 29-Datenschutzgruppe

Die Art. 29-Datenschutzgruppe ging bei den ersten beiden Kategorien von einer relativ sicheren Bestimmung der Verantwortlichkeit aus. Sie sollten um die 80% aller Verantwortlichkeitsszenarien abdecken. Trotz dieser Typologie müsste allerdings eine Überprüfung der expliziten oder impliziten Benennung des Verantwortlichen anhand der tatsächlichen Umstände erfolgen. Denn die Bestimmung des Verantwortlichen anhand formeller Kriterien sei aus zweierlei Gründen defizitär: Zum einen liege häufig keine Benennung eines Verantwortlichen vor,[310] zum anderen entspreche die formelle Zuweisung[311] häufig nicht den tatsächlichen Umständen.[312] Die eigentlich maßgebliche Kategorie des tatsächlichen Einflusses sieht die Art. 29-Datenschutzgruppe zudem kritisch im Hinblick auf die Komplexität der Analyse und das Risiko abweichender Bewertungen.[313]

Im Umkehrschluss zu den drei Kategorien der Typologie sah die Art. 29-Datenschutzgruppe schließlich die Benennung eines Verantwortlichen dann als unwirksam an, soweit dieser weder einen rechtlichen noch tatsächlichen Einfluss auf die Verarbeitung hat.[314]

---

[310] Dies soll per Gesetz, Vertrag oder Meldung an die Datenschutzbehörde möglich sein. Letzteres ist aufgrund des Wegfallens von Art. 18 DSRL und damit der Notifizierungspflicht als Konzept nicht mehr möglich. An dessen Stelle dürfte jetzt das Verfahrensverzeichnis nach Art. 30 DSGVO getreten sein, welches Aufsichtsbehörden aber nur auf Anfordern zu übermitteln ist.

[311] Die Art. 29-Datenschutzgruppe meint hier wohl die nicht-gesetzliche formelle Benennung.

[312] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[313] Vermutlich durch unterschiedliche Aufsichtsbehörden.

[314] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 15.

5. Kritik der Typologie

Auch wenn der Ansatz der Art. 29-Datenschutzgruppe zunächst durch seinen Pragmatismus besticht, verwundert es, dass die Art. 29-Datenschutzgruppe von ihrer anfangs proklamierten faktenbasierten Analyse in allen drei Kategorien zu einer Analyse anhand grundsätzlich formeller Kriterien kommt. Wie diese Kategorien den maßgeblichen tatsächlichen Einfluss dabei genau aufgreifen, bleibt weitestgehend unklar.

So ist es denkbar, dass die gesetzliche Festlegung einer Verantwortlichkeit den tatsächlichen Verhältnissen widerspricht.[315] Denkbar ist zudem, dass der Gesetzgeber eine singuläre Verantwortlichkeit vorsieht, tatsächlich aber gemeinsam Verantwortliche vorliegen. Wie solche Widersprüche aufzulösen wären, wird nicht ansatzweise angesprochen.[316] Es ist kein klarer Vorrang der gesetzlichen Festlegung gegenüber der tatsächlichen Verantwortlichkeit erkennbar. Zudem ist nicht klar, ob die tatsächliche Verantwortlichkeit möglicherweise Voraussetzung für eine gesetzliche Festlegung wäre. Nimmt man etwa an, dass die gesetzliche Festlegung einer singulären Verantwortlichkeit eine tatsächliche gemeinsame Verantwortlichkeit überschreibt, stellen sich Folgeprobleme auf der Ebene der Betroffenenrechte und aufsichtsbehördlicher Maßnahmen. Sofern sich der gesetzlich festgelegte Verantwortliche einen entsprechenden Einfluss gegenüber den tatsächlich Verantwortlichen verschaffen kann, wäre dies zwar unbedenklich,[317] problematisch erscheinen aber Szenarien, in denen der Gesetzgeber, bewusst oder unbewusst, Verantwortlichkeitskonstellationen schafft, die faktisch gar nicht durchführbar sind. Welchen Sinn dann die gesetzliche Fiktion einer Verantwortlichkeit haben würde, bleibt unklar. Eine sinnvolle Handhabung solcher Szenarien kann daher nur sein, dass sowohl der gesetzlich Verantwortliche wie auch der tatsächlich Verantwortliche einen Verantwortlichen im Sinne der Definition darstellen, gegebenenfalls dann auch gemeinsam Verantwortliche.

Auch dass der tatsächliche Einfluss primär anhand der vertraglichen Festlegungen festgestellt werden soll, läuft letztlich auf eine (quasi)-formalistische Feststellung der Verantwortlichen hinaus. Ausführliche Überlegungen zu Indikatoren für einen

[315] Für diesen Fall weist der EDPS nur darauf hin, dass die Benennung mit den tatsächlichen Verpflichtungen übereinstimmen soll: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 8 Fn. 6.

[316] A. in *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021 finden sich hierzu keinerlei Überlegungen.

[317] Insb., wenn dadurch die tatsächlich Verantwortlichen etwa zu Auftragsverarbeitern werden.

tatsächlichen Einfluss sind nicht vorhanden.[318] Die Aufstellung solcher Indikatoren mag in Anbetracht der Varianz potenzieller Faktoren sicher keine leichte Aufgabe sein. Allerdings findet sich nicht einmal ansatzweise ein Hinweis darauf, wie die Plausibilitätskontrolle der (quasi-)formellen Benennung in den verschiedenen Kategorien zu erfolgen hat. Selbst wenn es sich bei den drei Kategorien aufgrund des funktionellen Konzeptes der Verantwortlichkeit nur um eine Typologie handelt, wären aufgrund der Betonung der Erheblichkeit des tatsächlichen Einflusses dennoch Ausführungen hierzu zu erwarten gewesen. Die Art. 29-Datenschutzgruppe wollte ja selbst im Rahmen der Typologie einen pragmatischen und praktikablen Ansatz verfolgen. Letztlich erfolgt aber im Rahmen dieser Typologie keine, wenigstens abstrakte, Erläuterung des Definitionselements „entscheidet". Dies hat schwerwiegende Konsequenzen auch für die Feststellung einer gemeinsamen Verantwortlichkeit.

6. Verständnis des Europäischen Datenschutzbeauftragten (EDPS)

Ähnlich wie die Art. 29-Datenschutzgruppe analysiert auch der EDPS die Entscheidung anhand des tatsächlichen Einflusses über die Verarbeitung.[319] Dieser soll sich in der Ausübung der Entscheidungsmacht zeigen. Ausschlaggebend sollen dabei die folgenden Fragen sein:

- Warum findet die Verarbeitung statt?
- Wer hat die Verarbeitung begonnen?
- Wer profitiert von der Verarbeitung?

Ebenso wie die Art. 29-Datenschutzgruppe bildet der EDPS im Rahmen einer Typologie die Kategorien der ausdrücklichen rechtlichen Zuständigkeit und der implizierten Zuständigkeit. Beispielhaft für eine implizierte Zuständigkeit sollen die Aufgaben der European Medicines Agency, insbesondere im Hinblick auf Datenbanken, sein.[320] Daneben bildet auch der EDPS die Kategorie der tatsächlichen Zuständigkeit. Diese sei allerdings im Anwendungsbereich der VO (EU) 2018/1725, dem DSGVO-Äquivalent für die EU-Institutionen, kaum vorzufinden.

[318] Diese beschränken sich im Grunde auf einen Absatz: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 14 f.

[319] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 7 f.

[320] Siehe VO (EG) Nr. 726/2004.

Neben dem Kriterium der Entscheidung über die Zwecke und Mittel der Verarbeitung soll nach dem EDPS eine Stelle auch dann als Verantwortlicher gelten, wenn sie die Möglichkeit hat, die Verarbeitung zu beginnen und zu stoppen.[321] Letzteres scheint als isoliertes Kriterium allerdings untauglich, da auch der Auftragsverarbeiter häufig faktisch diese Möglichkeit hat. Die Möglichkeit die Verarbeitung zu beginnen und zu stoppen, sollte eher als Entscheidung über die wesentlichen Elemente der Mittel verstanden werden, gewissermaßen als wesentlichstes Element der Mittel. Damit wäre die Abgrenzung zum Auftragsverarbeiter unproblematisch, da dieser nicht über die wesentlichen Elemente der Mittel entscheiden darf. Tut er dies trotzdem, wird er aufgrund seines Auftragsverarbeiterexzesses[322] selbst zum Verantwortlichen gem. Art. 28 Abs. 10 DSGVO.

F. Benennung durch (materielles) Gesetz

Neben der Bestimmung des Verantwortlichen anhand der Definitionselemente selbst, kann dessen Benennung bzw. die dafür maßgeblichen Kriterien auch durch ein materielles Gesetz[323] erfolgen. So sieht Art. 4 Nr. 7 2. Hs. DSGVO vor:

*„[...]; sind die **Zwecke und Mittel dieser Verarbeitung** durch das **Unionsrecht** oder das **Recht der Mitgliedstaaten** vorgegeben, so kann der **Verantwortliche** beziehungsweise können die **bestimmten Kriterien seiner Benennung** nach dem **Unionsrecht** oder dem **Recht der Mitgliedstaaten** vorgesehen werden;“*[324]

Zwar zeigen sich hierbei gewisse Überschneidungen zur Typologie[325] der Art. 29-Datenschutzgruppe, allerdings handelt es sich bei dieser Typologie nur um eine Stellungnahme der Aufsichtsbehörden. Daneben bezieht die Art. 29-Datenschutzgruppe in ihre Typologie der ausdrücklichen rechtlichen Zuständigkeit zusätzlich auch die Verantwortlichkeit anhand einer Aufgabe oder Verpflichtung zum

[321] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 10.

[322] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[323] Gesetz bzw. gesetzlich im Rahmen dieses Kapitels meint immer ein materielles Gesetz bzw. materiell-gesetzlich.

[324] Hervorhebung durch den Autor.

[325] Dazu: Kapitel 2 E. V. Typologie anstatt formeller Analyse (Art. 29-Datenschutzgruppe / Europäischer Datenschutzausschuss).

Datenumgang ein. Dies wiederum gibt die Ermächtigung zur Benennung in Art. 4 Nr. 7 2. Hs. DSGVO nicht her. Daher ist eine isolierte Betrachtung dieser Ermächtigung notwendig.

Notwendige Voraussetzung für diese Spezifizierungsklausel ist die Festlegung der Zwecke und Mittel der Verarbeitung durch Unionsrecht oder das Recht eines Mitgliedstaats.[326] Ist dies erfolgt, kann der Verantwortliche entweder direkt oder aber können Kriterien für dessen Benennung im Unionsrecht oder dem Recht des Mitgliedstaats festgelegt werden. Nach Ansicht des EDPB können so auch mehrere Verantwortliche oder gemeinsam Verantwortliche benannt werden.[327]

I. Entstehungsgeschichte

Die Benennung des Verantwortlichen durch Unionsrecht oder das Recht der Mitgliedstaaten fand sich im ursprünglichen Entwurf der Kommission zur DSRL noch in einer etwas anderen Form. Für dessen Definition wurde die Definition des Verantwortlichen aus Art. 2 lit. d des ursprünglichen Übereinkommens Nr. 108 des Europarates im Wesentlichen übernommen.[328] Der Verantwortliche wurde durch Unionsrecht oder das Recht eines Mitgliedstaats benannt und war im Rahmen dieser Benennung dafür zuständig sein, „darüber zu entscheiden, welche Zweckbestimmung die Datei verfolgt, welche Arten personenbezogener Daten gespeichert und mit welchen Vorgängen sie verarbeitet werden sollen sowie welche Dritte Zugang zu den Dateien haben dürfen;".[329] Der abgeänderte Entwurf der Kommission kannte die Festlegung des Verantwortlichen durch Unionsrecht oder das Recht eines Mitgliedstaats hingegen nicht mehr. Die Möglichkeit der Benennung nach Unionsrecht oder dem Recht eines Mitgliedstaats tauchte erst wieder in der endgültigen Fassung der DSRL auf. Die DSGVO übernahm diesen Teil der Definition. Parallelen zum ursprünglichen Übereinkommen Nr. 108 des Europarates zwecks Auslegung der Norm lassen sich allerdings nur beschränkt ziehen, da die Benennung des Verantwortlichen in der DSGVO die Festlegung der Zwecke und Mittel der Verarbeitung per Gesetz, also eben nicht durch den Verantwortlichen, verlangt. Das modernisierte Übereinkommen Nr. 108 des Europarates, welches sich auch an der

[326] Zum Umsetzungsspielraum der Mitgliedstaaten: Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 27a.

[327] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 22.

[328] Zum Übereinkommen Nr. 108 des Europarates: Kapitel 1 B. IV. Übereinkommen Nr. 108 des Europarates (1981).

[329] BR-Drs. 690/90, S. 52 f.

DSGVO orientierte, enthält schließlich nun keine Möglichkeit der Festlegung des Verantwortlichen durch einzelstaatliches Recht mehr.

II. Bedeutung der Norm

Welche Art von Benennung der Unionsgesetzgeber mit dieser Spezifizierungsklausel genau intendiert hat, ist nicht ersichtlich. So räumte bereits die Art. 29-Datenschutzgruppe für die DSRL ein, dass eine solche ausdrückliche Benennung des Verantwortlichen nicht häufig erfolge.[330] Dass es sich bei der Benennung des Verantwortlichen durch Gesetz um ein reines Überbleibsel aus dem ursprünglichen Übereinkommen Nr. 108 des Europarates handelt, ist unwahrscheinlich. Denn die Benennung durch Gesetz war zwischenzeitlich nicht mehr vorgesehen und wurde mit ihrer Wiedereinführung in den Richtlinientext dann an zusätzliche Voraussetzungen geknüpft. Diese zusätzlichen Voraussetzungen kann man so verstehen, dass der Unionsgesetzgeber dem Unionsrecht sowie dem Recht der Mitgliedstaaten bestimmte Vorgaben machen wollte, damit der Verantwortliche nicht mehr völlig frei benannt werden konnte. Denn soweit Zwecke und Mittel der Verarbeitung dem Verantwortlichen durch Gesetz vorgegeben sind, kann dann die Entscheidung über diese nicht mehr als Kriterium für die Bestimmung des Verantwortlichen herhalten. Bei der Benennung des Verantwortlichen durch Gesetz handelt es sich dann nur noch um eine Aufgabenzuweisung.

III. Voraussetzungen der Benennung

Sinnvoll anwendbar erscheint die Festlegung der Verantwortlichkeit vor allem im Rahmen der Verarbeitungsrechtfertigungstatbestände Art. 6 Abs. 1 lit. c und lit. e DSGVO.[331] Denn bei der Umsetzung dieser Öffnungsklausel muss der Unions- oder mitgliedstaatliche Gesetzgeber aufgrund der rechtlichen Verpflichtung oder der Aufgabe zumindest indirekt die Zwecke der Verarbeitung festlegen. In diesem Zusammenhang kann der Gesetzgeber gleichzeitig auch die Mittel der Verarbeitung festlegen. Sofern dies erfolgt ist, lassen sich die Kriterien der Benennung des Verantwortlichen oder der Verantwortlichen selbst durch Gesetz festlegen.[332]

---

[330] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12. So sehen einige Mitgliedstaaten offensichtlich eine solche Benennung für Behörden im Rahmen ihres Aufgabenbereichs vor.

[331] Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 14; Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 24.

[332] Kritisch zu sehen wären daher wohl die Beispiele bei Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7

Wie bereits dargestellt, beinhalten die Mittel der Verarbeitung eine Reihe von unterschiedlichen Elementen.[333] Eine Festlegung sämtlicher Elemente der Mittel der Verarbeitung per Gesetz wäre daher sehr kleinteilig. Vernünftigerweise sollten deshalb nur die wesentlichen Elemente der Mittel[334] für eine gesetzliche Festlegung einbezogen werden, also etwa welche Daten von wem überhaupt verarbeitet werden sollen, für wie lange und wer Zugang zu ihnen hat. Die Festlegung konkreter Methoden der Verarbeitung, von einer bestimmten Soft- oder Hardware scheint hingegen in einem Gesetz kaum zielführend.[335] Denn dies würde langfristig eine flexible Handhabung der Verarbeitung durch den Verantwortlichen erschweren. Je nachdem, wie weitgehend man die notwendige Festlegung der Mittel per Gesetz versteht, führt dies zudem dazu, dass bestimmte bestehende gesetzliche Benennungen der Verantwortlichkeit bzw. der Kriterien hierfür rechtswidrig wären. Eine gesetzliche Benennung der Verantwortlichkeit kann im Rahmen der DSGVO nur dann Auswirkungen entfalten, wenn sie deren Voraussetzungen entspricht. Umso wichtiger ist es daher, konkrete Vorgaben zu den Voraussetzungen dieser Benennung zu machen. Dies würde de lege ferenda eine gesetzliche Ausdifferenzierung der Mittel bedingen. In jedem Fall wären Leitlinien des EDPB hilfreich.

Bei singulären Verantwortlichen ist die gesetzliche Festlegung des Verantwortlichen aufgrund der meist offensichtlichen Verantwortlichkeit häufig zu vernachlässigen. Zu denken wäre hier etwa an einen Arbeitgeber, der gewisse Daten für seine steuerlichen Pflichten erheben muss oder eine Behörde, die für die Genehmigung eines Antrags bestimmte Informationen benötigt. Sinnvoll ist die Festlegung der Verantwortlichkeit hingegen bei komplexen Verarbeitungsszenarien mit mehreren Akteuren. Dies gilt gerade auch für Auftragsverarbeitungen aufgrund der Festlegungserfordernisse in Art. 28 Abs. 3 DSGVO. Ebenso kann die Vereinbarung von gemeinsam Verantwortlichen gem. Art. 26 Abs. 1 S. 2 DSGVO auch durch gesetzliche Festlegungen ersetzt werden. So wäre etwa bei einer Datenbank oder gemeinsam betriebenen Plattformen daran zu denken, neben den Zwecken und Mitteln der Verarbeitung auch wenigstens die Kriterien zur Benennung der Verantwortlichen festzulegen. Denn hier kann aufgrund der Komplexität des Verarbeitungsszenarios gerade nicht mehr von einer offensichtlichen Erkennbarkeit der Verantwortlichkeiten ausgegangen werden.

DSGVO, Rn. 12, da dort direkt eine Verantwortlichkeit zugewiesen wird.

[333] Dazu: Kapitel 2 D. Mittel.

[334] Nach dem Verständnis der Art. 29-Datenschutzgruppe.

[335] Denkbar wäre eine solche Festlegung eventuell im Rahmen einer Verordnung (im deutschen Rechtssinne) oder durch Verwaltungsvorschriften.

Der EDPS sieht etwa Art. 57 der ETIAS-Verordnung[336] als eine Umsetzung von Art. 4 Nr. 7 2. Hs. DSGVO.[337] Dort wird die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems geregelt. In der Literatur finden sich selten genauere Ausführungen zur gesetzlichen Festlegung der Verantwortlichkeit. *Dammann* etwa schlug für die DSRL vor, diese Möglichkeit für die Regelung der Verantwortlichkeit bei Verbundsystemen, Chipkartensystemen oder Mailboxen zu nutzen.[338] *Brühann* wiederum sah bestimmte öffentliche Register als Anwendungsfall.[339]

Im Januar 2024 entschied der EuGH erstmal zu der gesetzlichen Benennung eines Verantwortlichen.[340] Aufgrund der weiten Definition des Verantwortlichen könne die Vorgabe der Zwecke und Mittel der Verarbeitung und gegebenenfalls auch die Benennung des Verantwortlichen durch das nationale Recht nicht nur explizit, sondern auch implizit erfolgen.[341] Wenn sie implizit erfolge, sei es jedoch erforderlich, dass sich diese Vorgabe mit hinreichender Bestimmtheit aus der Rolle, dem Auftrag und den Aufgaben der betroffenen Person oder Einrichtung ergebe. Eine explizite Vorgabe sei zum Schutz dieser (verantwortlichen) Personen nicht zwingend erforderlich. Durch nationales Recht könne schließlich auch eine gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO im Sinne einer Kette von Verarbeitungen vorgegeben werden.[342] Eine solche Kette von Verarbeitungen könne sich implizit aus dem nationalen Recht ergeben, müsse dann aber auch hinreichend deutlich erkennbar sein.[343] Die Möglichkeit einer impliziten Vorgabe hat zwar den Charm einer gewissen Flexibilität, sie wirft aber zahlreiche Folgefragen auf und dürfte weitere EuGH-Entscheidungen nach sich ziehen.

IV. Qualifizierte Verantwortlichkeit als Benennung?

Fraglich erscheint im Zusammenhang mit der gesetzlichen Benennung des Verantwortlichen, ob die Qualifizierung eines Verantwortlichen anhand von Begriffen

[336] VO (EU) 2018/1240.

[337] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 8.

[338] Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 14.

[339] Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 21.

[340] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265.

[341] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265, Rn. 30.

[342] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265, Rn. 45 ff.

[343] EuGH, Urteil vom 11.01.2024 – C-231/22 (État belge) = EuZW 2024, 265, Rn. 50.

wie „übermittelnde“[344] oder „speichernde“ eine Benennung des Verantwortlichen oder seiner Kriterien darstellt. Ohne zusätzliche gesetzliche Vorgaben bezüglich der Zwecke und Mittel der Verarbeitung ist dies aber nicht der Fall.[345] Die reine Qualifizierung eines Verantwortlichen bedeutet regelmäßig keine damit einhergehende Festlegung von Zwecken und Mitteln. So sagt etwa die Qualifizierung „übermittelnd“ nur etwas über die Form der Verarbeitung aus. Somit werden anhand dieser Qualifizierung vielmehr nur die für die Verantwortlichkeit relevanten Verarbeitungsvorgänge eingegrenzt. Dies kann insbesondere in Verarbeitungsszenarien mit mehreren Akteuren aus Klarstellungsgründen sinnvoll sein, ist aber für die Benennung des Verantwortlichen insgesamt unerheblich.

V. Übernahme der Normadressaten aus anderen Rechtsgebieten

Denkbar erscheint es zunächst, die zentralen Normadressaten aus anderen Rechtsgebieten für das Datenschutzrecht zu übernehmen. Die Art. 29-Datenschutzgruppe weist allerdings darauf hin, dass der Verantwortliche im Datenschutzrecht autonom von externen Rechtsquellen, insbesondere anderen Rechtsgebieten, bestimmt werden sollte.[346] Zwar könnten solche Quellen zur Feststellung des Verantwortlichen beitragen, allerdings solle die Analyse der Verantwortlichkeit grundsätzlich unbeeinflusst von datenschutzfremden Begriffen wie etwa dem Urheber, Rechteinhaber oder dem Begriff der Haftung erfolgen. Denn datenschutzfremde Begriffe können sowohl Gegensätze wie auch Schnittmengen zu bzw. mit dem Verantwortlichen darstellen. In jedem Fall würden sie keinen notwendigen Schluss auf die Verantwortlichkeit bedingen. Im Hinblick auf die Benennung des Verantwortlichen bzw. seiner Kriterien erscheint es zudem sehr unwahrscheinlich, dass ein anderes Rechtsgebiet die Zwecke und Mittel der Verarbeitung in ausreichender Weise festlegt.

[344] § 74 BDSG (Art. 3 Abs. 8 DSRL-JI enthält ebenso wie die DSGVO eine entsprechende Spezifizierungsklausel).

[345] Vgl. Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 13, der die begriffliche Vielfalt des BDSG a.F. nur im Hinblick auf die Vereinbarkeit mit der DSRL betrachtet.

[346] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12.

VI. Vorrang der tatsächlichen Verantwortlichkeit gegenüber der rechtlichen?

Unklar ist schließlich, wie mit der Situation umzugehen wäre, wenn eine gesetzliche Benennung der Verantwortlichkeit nicht den tatsächlichen Verhältnissen entsprechen würde. Die Art. 29-Datenschutzgruppe deutet an, dass eine tatsächliche Verantwortlichkeit eine formelle Verantwortlichkeit überschreiben könnte.[347] Allerdings wird dabei nicht klar, ob mit der formellen Benennung ausschließlich eine interne Zuschreibung des Verantwortlichen gemeint ist oder zusätzlich auch eine gesetzliche Benennung erfasst wäre. Ausgehend vom Wortlaut von Art. 4 Nr. 7 2. Hs. DSGVO dürfte kein Vorrang der tatsächlichen Verantwortlichkeit gegenüber einer gesetzlichen Benennung bestehen. Sind die Zwecke und Mittel einer Verarbeitung per Gesetz bestimmt, kann der benannte[348] Verantwortliche nicht mehr über diese entscheiden. Es bedarf also gerade einer anderweitigen Zuweisung der Verantwortlichkeit, da die Bestimmung nach den tatsächlichen Umständen nicht möglich ist. Der Verantwortliche ist in diesem Fall sozusagen weisungsgebunden gegenüber der gesetzlichen Festlegung der Zwecke und Mittel der Verarbeitung. Ein Auseinanderfallen von gesetzlicher Benennung und tatsächlicher Verantwortlichkeit ist demnach nur denkbar für den Fall, dass der durch Gesetz benannte Verantwortliche sich über die gesetzliche Festlegung der Zwecke und/oder Mittel hinwegsetzt. Analog zum Auftrags- und Mitarbeiterexzess könnte man hier vom gesetzlichen Verantwortlichenexzess sprechen. Welche Konsequenzen dies haben könnte, ist aber unklar. Verantwortlich wäre im Zweifel immer noch dieselbe Stelle. Denkbar wären im öffentlich-rechtlichen Bereich Ausnahmen von der Staatshaftung im Sinne einer persönlichen Haftung des Entscheidungsträgers sowie disziplinarische Konsequenzen. Sofern man eine rechtliche Festlegung der Verantwortlichkeit im nicht-öffentlichen Bereich, abseits der Beleihung und des Verwaltungshelfers annimmt, scheinen die Konsequenzen dort völlig unklar.

Plastisch wird das Spannungsverhältnis zwischen gesetzlicher Benennung der Verantwortlichkeit und tatsächlicher Verantwortlichkeit vor allem in Verarbeitungsszenarien mit mehreren Akteuren. So ist das Szenario denkbar, dass ein Akteur gesetzlich als Verantwortlicher benannt ist, er seine Verarbeitungen aber tatsächlich zusammen mit anderen Akteuren durchführt, die allerdings nicht gesetzlich benannt sind. Die fehlende gesetzliche Benennung der anderen Akteure wäre dann

[347] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[348] Bzw. der anhand der Kriterien benannte Verantwortliche.

unproblematisch, wenn es sich bei diesen um Auftragsverarbeiter handelt. Denn eine Sperrwirkung gegenüber einer Auftragsverarbeitung durch Dritte aufgrund der gesetzlichen Benennung eines Verantwortlichen ist nicht ersichtlich. Soweit es sich bei diesen anderen Akteuren allerdings nicht um Auftragsverarbeiter handelt und aufgrund der tatsächlichen Umstände eine gemeinsame Verantwortlichkeit zwischen dem gesetzlich benanntem Verantwortlichen und den anderen Akteuren vorliegt, ist unklar, welche Auswirkungen dies hat. Denkbar ist auf der einen Seite, dass aufgrund der Festlegung eines singulären Verantwortlichen die anderen Akteure gar nicht gemeinsam Verantwortliche sein können, da das Gesetz nur diesen einen Verantwortlichen benennt. Auf der anderen Seite ist denkbar, dass durch die tatsächliche gemeinsame Verantwortlichkeit die singuläre Verantwortlichkeit des gesetzlich benannten Verantwortlichen überschrieben wird.[349] Problematisch erweist sich bei letzterem Verständnis allerdings, dass die anderen Akteure aufgrund der gesetzlichen Festlegung der Zwecke und Mittel der Verarbeitung im Rahmen der gesetzlichen Benennung des Verantwortlichen eigentlich keinen Entscheidungsbeitrag[350] erbringen können. Denn das Gesetz legt die Zwecke und Mittel der Verarbeitung abschließend fest. Denkbar wäre noch ein Zu-Eigen-Machen[351] der Zwecke und/oder Mittel der Verarbeitung durch die anderen Akteure. Allerdings könnte dies immer noch mit der gesetzlichen Benennung im Widerspruch stehen, da diese ja nur einen singulären Verantwortlichen vorsieht. Schließlich könnte ein Verantwortlichenexzess dahingehend vorliegen, dass der gesetzlich benannte Verantwortliche die gemeinsame Verantwortlichkeit zugelassen hat. Auch dies könnte dann die gesetzliche Benennung überschreiben. Gerade in Verarbeitungsszenarien mit potenziell mehreren Akteuren scheint daher eine gesetzliche Festlegung der Kriterien für die Benennung eines Verantwortlichen gegenüber der direkten Benennung sinnvoller. Dies lässt sich auch unproblematisch mit der gesetzlichen Festlegung der Verteilung der Pflichten gem. Art. 26 Abs. 1 S. 2 DSGVO vereinbaren. Allerdings setzt dies, ebenso wie die direkte Benennung von gemeinsam Verantwortlichen, eine entsprechende Weitsicht des Gesetzgebers voraus.

Kommt es zu einem Widerspruch zwischen gesetzlicher Benennung der Verantwortlichen und tatsächlicher Bestimmung der Verantwortlichen ist im Zweifel der gesetzlichen Benennung Vorrang einzuräumen. Denn in diesem Fall fehlt es an

[349] Simitis/Hornung/Spiecker/*Petri*, Art. 4 Nr. 7 DSGVO, Rn. 26 möchte dabei den Rechtsgedanken aus Art. 26 Abs. 2 DSGVO anwenden.

[350] Dazu: Kapitel 4 I. Erheblichkeitsschwelle des Entscheidungsbeitrags.

[351] Dazu: Kapitel 4 G. III. Zu-Eigen-Machen als Billigung oder Entscheidung?

einer Kollisionsregel. Sofern möglich, wäre dann eine parallele Verantwortlichkeit der eigentlich gemeinsam Verantwortlichen anzunehmen.

VII. Anwendungsfälle?

Die folgenden Normen bilden potenzielle Anwendungsfälle für die gesetzliche Benennung des Verantwortlichen nach Art. 4 Nr. 7 2. Hs. DSGVO. Dabei ist die Analyse, ob der Gesetzgeber damit tatsächlich die Spezifizierungsklausel der DSGVO umsetzen will, nicht trivial. Denn zum einen findet sich, soweit ersichtlich, nie ein Hinweis auf Art. 4 Nr. 7 2. Hs. DSGVO in der Gesetzesbegründung und zum anderen liegt kaum Literatur vor, die sich hiermit befasst.

1. TKG

Ein denkbarer Anwendungsfall für die gesetzliche Benennung eines Verantwortlichen könnte etwa §§ 172 f. TKG sein. § 172 TKG regelt, dass bestimmte Daten durch Telekommunikationsdiensteanbieter für Auskunftsersuche gegenüber Sicherheitsbehörden erhoben und gespeichert werden müssen. § 173 TKG wiederum regelt das automatisierte Auskunftsverfahren gegenüber diesen Sicherheitsbehörden. Die Verpflichteten ergeben sich aus § 173 Abs. 1 S. 1 i.V.m. § 172 Abs. 1 TKG und sind primär Stellen, die Telekommunikationsdienste erbringen. Diese sind, wie sich aus § 173 Abs. 1 S. 1 i.V.m. § 172 Abs. 1 TKG ergibt, jedenfalls für die Erhebung und Speicherung der Daten verantwortlich. Dabei kann gem. § 173 Abs. 1 S. 2 TKG auch ein Auftragsverarbeiter gem. Art. 28 DSGVO beauftragt werden. Die Verantwortlichkeit der Verpflichteten bleibt allerdings auch bei Einschaltung von Dritten gem. § 172 Abs. 5 TKG bestehen. Für die weitere Übermittlung[352] der Daten nach Abruf durch die Bundesnetzagentur ist entweder diese gem. § 173 Abs. 7 S. 3 Nr. 1 TKG selbst verantwortlich oder gem. § 173 Abs. 7 S. 3 Nr. 2 TKG die in § 173 Abs. 4 genannten Stellen, die Auskunft ersuchen. Die Bundesnetzagentur muss daher auch gem. § 173 Abs. 8 TKG die Abrufe protokollieren. Die zu speichernden Daten ergeben sich aus § 173 Abs. 1 S. 1 i.V.m. § 172 Abs. 1, 2 und 4 TKG. Die Speicherdauer ergibt sich aus der Pflicht zur Löschung gem. § 173 Abs. 1 S. 3 i.V.m. § 172 Abs. 6 TKG. Die Pflicht zur Berichtigung ergibt sich aus § 173 Abs. 1 S. 3 i.V.m. § 172 Abs. 4 TKG. Technische Vorgaben für den Verpflichteten ergeben sich aus § 173 Abs. 9 TKG sowie für den Abruf der Daten aus § 173 Abs. 2 TKG. Weitere technische Vorgaben ergeben sich aus der Rechtsverordnung die gem. § 173 Abs. 5 TKG erlassen werden kann sowie aus der technischen Richtlinie gem. § 173

[352] Sinnvollerweise scheint damit der Abruf gemeint.

Abs. 6 TKG. Zwar liegt hier noch keine direkte Benennung des Verantwortlichen i.S.v. Art. 4 Nr. 7 2. Hs. 1. Var. DSGVO vor („Wer [...] erbringt [...]), allerdings sind die Kriterien seiner Benennung i.S.v. Art. 4 Nr. 7 2. Hs. 2. Var. DSGVO vorhanden.

2. MsbG

Das Messstellenbetriebsgesetz (MsbG) regelt den Markt für den Betrieb von Messstellen und die Ausstattung der leitungsgebundenen Energieversorgung mit modernen Messeinrichtungen und intelligenten Messsystemen. § 49 MsbG listet in Abs. 2 i.V.m. Abs. 1 S. 1 diejenigen Stellen auf, die im Rahmen des Gesetzes personenbezogene Daten verarbeiten dürfen. Dabei handelt es sich um die sogenannten berechtigten Stellen.[353] Diese berechtigten Stellen können nach § 49 Abs. 3 MsbG die Verarbeitung auch durch Auftragsverarbeiter gem. Art. 28 DSGVO durchführen lassen. Dabei ergeben sich die Zwecke der Verarbeitung aus § 50 MsbG. Die Mittel der Verarbeitung ergeben sich aus §§ 51 ff. MsbG und dabei insbesondere aus §§ 55-59 MsbG. Bei diesen berechtigten Stellen handelt es sich also um gesetzlich benannte Verantwortliche.

3. StVG

Deutlich weniger klar ist bei § 63a StVG, ob eine gesetzliche Benennung des Verantwortlichen erfolgt. Diese Norm soll, wie sich aus ihrem Titel ergibt, die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion regeln. In § 63a Abs. 1 StVG wird festgelegt, wann ein Kraftfahrzeug mit hoch- oder vollautomatisierter Fahrfunktion Positions- und Zeitangaben wegen eines Wechsels der Fahrzeugsteuerung von oder zum Fahrzeugführer speichert. Eine Speicherung soll ebenso erfolgen, wenn das System den Fahrzeugführer zur Übernahme der Steuerung auffordert oder eine technische Störung des Systems auftritt. § 63a Abs. 4 StVG regelt die Dauer der Speicherung, § 63a Abs. 2 S. 3 StVG den Umfang der zu speichernden Daten. Bei Dauer und Umfang der Speicherung handelt es um wesentliche Elemente der Mittel. § 63a Abs. 2 S. 1, Abs. 3, 5 StVG wiederum regeln die potenziellen Zwecke der Verarbeitung: die Kontrolle von Verkehrsverstößen durch die zuständigen Behörden, die Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen sowie die Unfallforschung.

Der zur Speicherung Verpflichtete selbst wird in § 63a Abs. 2 StVG allerdings nicht deutlich. So dürfen die gemäß Abs. 1 gespeicherten Daten den nach Landesrecht für

[353] BerlKommEnR/*Lindermann*, § 49 MsbG, Rn. 22.

die Ahndung von Verkehrsverstößen zuständigen Behörden auf deren Verlangen hin zwar übermittelt werden, doch durch wen diese Übermittlung erfolgen soll, ist § 63a Abs. 2 StVG nicht zu entnehmen. Denkbar ist, dass der in § 63a Abs. 3 StVG erwähnte Fahrzeughalter gemeint ist. Dieser soll für die Fälle des § 63a Abs. 3 StVG die Übermittlung allerdings nur veranlassen. Ob er daher tatsächlich Verantwortlicher ist, ist zweifelhaft.[354] Klarstellung könnte der mittlerweile verabschiedete § 1g StVG bringen. Dieser verpflichtet den Halter eines Kraftfahrzeugs mit autonomer Fahrfunktion, verschiedene Daten gem. § 1g Abs. 1 S. 1 StVG beim Betrieb des Kraftfahrzeugs zu speichern. Ebenso verpflichtet § 1g Abs. 1 S. 2 StVG zur Übermittlung der Daten nach S. 1 an das Kraftfahrt-Bundesamt und an nach Landesrecht zuständige Behörden. § 1 Abs. 2 StVG nennt die konkreten Anlässe für die Speicherung nach Abs. 1. Die Begründung für den Entwurf des § 1g StVG bestätigt zudem, dass der Halter Berechtigter für die anfallenden Daten sein soll.[355]

4. ATDG

Eine gesetzliche Benennung des Verantwortlichen kann man auch in § 8 ATDG erkennen.[356] Diese Norm regelt die datenschutzrechtliche Verantwortung im Rahmen der Führung der Antiterrordatei. Die Norm unterfällt zwar nicht insgesamt dem Anwendungsbereich der DSGVO, jedoch gilt zumindest für die beteiligten Polizeibehörden[357] die DSRL-JI.[358] Entsprechend zur DSGVO definiert die DSRL-JI in Art. 3 Nr. 8 DSRL-JI den Verantwortlichen sowie in Art. 21 DSRL-JI die gemeinsam Verantwortlichen fast identisch.[359] Die relevanten Ausführungen zur DSGVO greifen also auch für die DSRL-JI. Gem. § 8 Abs. 1 S. 1 ATDG ist die Behörde,

---

[354] Kritisch bereits zum Entwurf *Piltz*, https://www.delegedata.de/2017/02/gesetzentwurf-zum-automatisierten-fahren-datenschutzrechtlich-mangelhaft/ (abgerufen am 17.07.2024); vgl. a. die Stellungnahme des Bundesrates sowie die Antworten der Bundesregierung zum Entwurf: *Deutscher Bundestag*, https://dserver.bundestag.de/btd/18/115/1811534.pdf (abgerufen am 17.07.2024) S. 6 ff.

[355] *Bundesregierung*, https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile (abgerufen am 17.07.2024) S. 42: „Die Regelung basiert auf dem Verständnis, dass die Halterinnen und Halter die Berechtigten hinsichtlich der Daten sind, die beim Betrieb des Kraftfahrzeugs in autonomer Fahrfunktion anfallen, und dass die Hersteller die Ausübung der Datenhoheit technisch und organisatorisch ermöglichen müssen."

[356] *Radtke*, JIPITEC[11] (2020), 242, Rn. 20.

[357] Also des BKAs, der bestimmten Bundespolizeibehörden, der LKAs sowie des Zollkriminalamts.

[358] Art. 1 Abs. 1 DSRL-JI: „Diese Richtlinie enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit."

[359] Zur gemeinsamen Verantwortlichkeit in der DSRL-JI: *Radtke*, JIPITEC[11] (2020), 242.

die Daten in die Antiterrordatei eingegeben hat, Verantwortlicher.[360] Dabei soll die Behörde, die die Daten eingegeben hat, erkennbar sein. Die Verantwortung für die Zulässigkeit einer Abfrage soll gem. § 8 Abs. 1 S. 3 ATDG hingegen nicht die eingebende, sondern die abfragende Behörde tragen. Daneben darf gem. § 8 Abs. 2 ATDG nur die Behörde, die die Daten eingegeben hat, diese Daten ändern, berichtigen, in ihrer Verarbeitung einschränken oder löschen. Sollten die Daten unrichtig sein, kann die eingebende Behörde gem. § 8 Abs. 3 ATDG auf eine Aufforderung und Prüfung hin die Daten berichtigen. Zuständig für die Protokollierung der Zugriffe sowie die technischen und organisatorischen Maßnahmen ist nach § 9 ATDG das Bundeskriminalamt. Der Zweck der Verarbeitung im Rahmen der Antiterrordatei ergibt sich dabei aus § 1 Abs. 1 ATDG durch die Aufklärung oder Bekämpfung des internationalen Terrorismus. Die Mittel der Verarbeitung ergeben sich wiederum aus §§ 2 ff. ATDG.

Grundsätzlich sollte bei solchen gemeinsamen Dateien[361] zwischen drei wesentlichen Verarbeitungsvorgängen unterschieden werden. Dies ist zum einen die Eingabe oder die Änderung von Daten in der gemeinsamen Datei. Die Verantwortlichkeit hierfür kann nur bei der eingebenden bzw. ändernden Stelle liegen, so auch § 8 Abs. 1 S. 1 ATDG. Denn eine Prüfung der Eingabe oder Änderung durch andere Stellen kann erst dann erfolgen, wenn sie bekannt ist. Daneben stellt die Abfrage bzw. Erhebung aus der gemeinsamen Datei einen separaten Vorgang dar, für den nur die abfragende Stelle verantwortlich sein kann, so auch § 8 Abs. 1 S. 3 ATDG. Denn eine Prüfung der Zulässigkeit der Abfrage könnte nur eingeschränkt durch den Betreiber der gemeinsamen Datei vorgenommen werden. Letztlich stellt aber auch die Speicherung der Daten in der Datei einen isolierbaren Vorgang dar. Für diese Speicherung der Daten erscheint § 12 ATDG als sehr eindeutiger Hinweis auf eine gemeinsame Verantwortlichkeit.[362] Nach dieser Norm hat das Bundeskriminalamt für die gemeinsame Datei im Einvernehmen mit den beteiligten Behörden bestimmte Einzelheiten festzulegen.[363] Dazu gehören etwa

---

[360] Vgl. a. § 31 Abs. 2 BKAG.

[361] Siehe zu weiteren Anwendungsfällen: BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 91b ff.

[362] Vgl. auch die mittlerweile zurückgezogene EuGH-Vorlage zum INPOL-System: VG Wiesbaden, Beschluss vom 30.07.2021 – 6 K 421/21 = CR 2021, 732. Zur Rücknahme: *Schild*, ZD-Aktuell 2022, 01264.

[363] Zusätzlich zur Festlegung bedarf es a. noch der Zustimmung des Bundesministeriums des Innern, für Bau und Heimat, des Bundeskanzleramts, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen und der für die beteiligten Behörden der Länder zuständigen obersten Landesbehörden.

- die Art der zu speichernden Daten nach § 3 Abs. 1 ATDG,
- die Eingabe der zu speichernden Daten,
- die zugriffsberechtigten Organisationseinheiten der beteiligten Behörden und
- die Protokollierung.

Dabei dürften all diese Punkte der Festlegung der Mittel den wesentlichen Elementen der Mittel unterfallen.[364] Daher wäre jedenfalls für den Vorgang der Speicherung, mit anderen Worten also dem Betrieb einer gemeinsamen Datei, eine gemeinsame Verantwortlichkeit anzunehmen.[365]

Ein weiterer Ansatzpunkt für eine Verantwortlichkeit könnte allerdings auch die Berichtigung unrichtiger Daten durch die eingebende Stelle nach Hinweis einer anderen Stelle und die darauffolgende Prüfung sein. Sofern es sich nur um eine Korrektur offensichtlicher Eingabe- oder ähnlicher formeller Fehler handelt, ist dies im Hinblick auf die Verantwortlichkeit zwar unproblematisch. Sofern mit einer solchen „Berichtigung" aber eine Erweiterung oder eine inhaltliche Änderung der Daten verbunden ist, ist hier zumindest eine gemeinsame Verantwortlichkeit der eingebenden bzw. ändernden Stelle zusammen mit der anderen hinweisenden Stelle für diesen Datensatz anzunehmen. Von der singulären Verantwortlichkeit der eingebenden bzw. ändernden Stelle aufgrund der tatsächlichen Änderung, trotz des Hinweises der anderen Stelle auszugehen, wäre reiner Formalismus.[366]

5. BVerfSchG

Eine ähnliche Regelung wie in § 8 ATDG findet sich in § 6 Abs. 2 S. 5 BVerfSchG. § 6 Abs. 2 BVerfSchG regelt die gegenseitige Unterrichtung der Verfassungsschutzbehörden durch gemeinsame nachrichtendienstliche Informationssysteme. Die DSRL-JI findet allerdings mangels Anwendungsbereichs für

[364] Vgl. dazu a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 2 (Forschungsinstitute) zur positiven Abgrenzung sowie zur negativen Abgrenzung ebd., Rn. 71 Beispiel 1. Letzteres Beispiel setzt voraus, dass die Akteure allein über die wesentlichen Elemente der Mittel entscheiden und die Daten der anderen Akteure nicht abrufen oder nutzen können.

[365] Vgl. Auernhammer/*Eßer*, Art. 4 DSGVO, Rn. 79.

[366] Unklar etwa die normative Aufhängung der „Mitprüfungspflicht" bei: *Riegel*, 8.4 Datenschutz bei den Nachrichtendiensten, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 95 ff.

den nachrichtendienstlichen Bereich[367] nur über den Bezug auf die allgemeinen Vorschriften des Datenschutzrechts und somit auf das BDSG entsprechende Anwendung. Über das BDSG und die darin erfolgte Umsetzung der DSRL-JI findet die DSRL-JI also indirekt Anwendung. Die Zwecke und Mittel der Verarbeitung finden sich in §§ 10 f. BVerfSchG sowie § 6 BVerfSchG selbst. In § 6 Abs. 2 S. 5 BVerfSchG wird die Verantwortlichkeit für die Daten in den gemeinsamen Dateien (der Landesbehörden für Verfassungsschutz und des Bundesamtes für Verfassungsschutz) trotz einer denkbaren gemeinsamen Verantwortlichkeit den jeweils eingebenden Stellen zugewiesen. Demnach dürfen nur diese die von ihnen eingegebenen Daten verändern, löschen oder deren Verarbeitung einschränken.[368]

Diese Festlegung der Verantwortlichkeit mag dem System einer Verbunddatei[369] entsprechen, allerdings wäre nach datenschutzrechtlichem Verständnis eine getrennte Verantwortlichkeit eher noch bei einer Zentraldatei anzunehmen.[370] Neben dem Dateityp der Verbunddatei spricht auch die Wahrnehmung der technischen und organisatorischen Maßnahmen für die gemeinsamen Dateien durch das BfV gegen eine getrennte Verantwortlichkeit. Dies gilt auch abseits einer inhaltlichen Prüfung der eingegebenen Daten durch das BfV.[371]

G. Der Auftragsverarbeiter als Abgrenzungsobjekt

I. Allgemeine Voraussetzungen

Im Hinblick auf die Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter ist neben der Kenntnis der Definitionselemente des Verantwortlichen zumindest auch ein grobes Verständnis des Auftragsverarbeiters notwendig.[372] Denn gerade die

[367] Kritisch: BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, Rn. 9a, d.

[368] Unklar ist dabei, ob es für identische Personen dann mehrere Dateien verschiedener Verfassungsschutzbehörden gibt oder ob die zuständige Verfassungsschutzbehörden auf Zuruf einen Datensatz ergänzen bzw. verändern. Der Wortlaut von § 6 Abs. 2 BVerfSchG dürfte gegen letzteres sprechen. Andererseits handelt es sich nicht mehr um reine Hinweisdateien, vgl. Schenke/Graulich/Ruthig/*Roth*, § 6 BVerfSchG, Rn. 21, 31.

[369] Vgl. für die Dateitypen Schenke/Graulich/Ruthig/*Roth*, § 6 BVerfSchG, Rn. 1 f.

[370] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 26.

[371] Vgl. Schenke/Graulich/Ruthig/*Roth*, § 6 BVerfSchG, Rn. 35 f.

[372] Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 238. Allgemein zur Bedeutung des Auf-

Abgrenzung zwischen Auftragsverarbeiter und gemeinsam Verantwortlichem als weiteres Szenario mit mehreren Akteuren ist ungemein wichtig.[373]

Der Auftragsverarbeiter wurde im ursprünglichen Übereinkommen Nr. 108 des Europarates nicht erwähnt.[374] Allerdings war die „Verarbeitung im Auftrag" im deutschen Datenschutzrecht bereits seit dem BDSG 1977 in § 8 als Konzept vorhanden. In der DSRL wurde der Auftragsverarbeiter erst im abgeänderten Vorschlag der Kommission zur DSRL ausdrücklich definiert.[375] Im Rahmen der DSGVO wurde dem Auftragsverarbeiter erstmalig selbst, also nicht indirekt über den Verantwortlichen, eine Reihe von Pflichten auferlegt.[376] Der Auftragsverarbeiter ist gem. Art. 4 Nr. 8 DSGVO:

> *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;".*

Ausgehend von dieser Definition lassen sich zunächst drei Definitionselemente isolieren:

- eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle (**personenbezogener Aspekt**),
- die im Auftrag des Verantwortlichen (**Abgrenzungsaspekt**)
- (personenbezogene Daten) verarbeitet (**Anwendungsbereich**).

Hinsichtlich des personenbezogenen Aspektes wird auf die Erörterungen in Kapitel 2. B.[377] verwiesen.[378] Die Verarbeitung personenbezogener Daten beschreibt wie auch beim Verantwortlichen den Anwendungsbereich des Datenschutzrechts überhaupt

tragsverarbeiter: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 7; *Alsenoy*, CLSR[28] (2012), 25, 29.

[373] Vgl. Kühling/Buchner/*Hartung*, Art. 28 DS-GVO, Rn. 26 ff. Siehe zum Vorgehen auch: *Marx/Sütthoff*, CR 2023, 29, 33.

[374] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5, 30.

[375] BT-Drs. 12/8329, S. 67.

[376] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 93. Detaillierter: *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 48 ff., 55.

[377] Dazu: Kapitel 2 B. Stelle.

[378] Vgl. a. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 30. Ebenso: Kühling/Buchner/*Hartung*, Art. 4 Nr. 8 DS-GVO, Rn. 6.

und ist daher hier nicht von spezifischem Interesse.[379] Hervorzuheben ist allerdings, dass der Auftragsverarbeiter gemäß seiner Definition nicht über die Verarbeitung entscheidet, sondern sie schlicht durchführt.[380]

Ausgehend von seiner Definition scheint das wesentliche Abgrenzungsmerkmal des Auftragsverarbeiters zum Verantwortlichen also, dass er „im Auftrag des Verantwortlichen" zu handeln hat. Die Definition enthält damit keine eigenständigen Elemente, die einen Auftragsverarbeiter charakterisieren.[381] Die Abgrenzung zum Verantwortlichen erfolgt vielmehr danach, dass ein Auftragsverarbeiter aufgrund der Entscheidung eines Verantwortlichen zu dessen Beauftragung die Verarbeitung durchführt. Der Verantwortliche hat bei der Durchführung einer Verarbeitung ein Ermessen dergestalt, dass er die Daten entweder innerhalb seiner Organisationseinheit durch die ihm unterstellten Personen verarbeiten lassen kann oder er die Verarbeitung ganz oder teilweise an externe Stellen delegiert. Diese Delegation der Verarbeitung an externe Stellen erfolgt im Interesse und auf Weisung des Verantwortlichen. Die Entscheidungshoheit hinsichtlich der Zwecke und wesentlichen Elemente der Mittel verbleiben dabei beim Verantwortlichen.

Der Auftragsverarbeiter wird neben der Definition in Art. 4 Nr. 8 DSGVO in Art. 28 DSGVO näher geregelt.[382] Art. 28 Abs. 1 DSGVO macht dem Verantwortlichen dabei bestimmte Vorgaben für die Auswahl des Auftragsverarbeiters. Der Auftragsverarbeiter soll „[...] hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet."[383] Art. 28 Abs. 2 DSGVO regelt die Frage, ob und unter welchen Voraussetzungen der Auftragsverarbeiter wiederum seinerseits Auftragsverarbeiter einsetzen darf und macht dies von der Genehmigung des Verantwortlichen abhängig.[384] Kernstück von Art. 28 DSGVO ist vor allem Abs. 3 S. 1. Demnach erfolgt die Verarbeitung des Auftragsverarbeiters auf Grundlage eines Vertrags oder eines anderen

[379] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 79.

[380] Er „verarbeitet".

[381] Kühling/Buchner/*Hartung*, Art. 4 Nr. 8 DS-GVO, Rn. 7.

[382] Dies wird ergänzt durch ErwGr 81 DSGVO.

[383] Dazu: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 94 ff.

[384] Bzw. bei einer allgemeinen Genehmigung von entsprechenden Informationen des Auftragsverarbeiters an den Verantwortlichen. Dazu: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 151 ff.

Rechtsinstruments nach dem Unionsrecht[385] oder dem Recht der Mitgliedstaaten.[386] Diese Instrumente binden den Auftragsverarbeiter in Bezug auf den Verantwortlichen und legen folgende Elemente fest:[387]

- Gegenstand der Verarbeitung
- Dauer der Verarbeitung
- Art der Verarbeitung
- Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Personen
- Pflichten und Rechte des Verantwortlichen

Dabei kann man bis auf den Zweck der Verarbeitung und die Pflichten und Rechte des Verantwortlichen all diese Festlegungen auch als wesentliche Elemente der Mittel[388] verstehen.

Maßgeblich ist für den Auftragsverarbeiter neben diesen Festlegungen vor allem Art. 28 Abs. 3 lit. a DSGVO. Demnach sieht der Vertrag bzw. das Rechtsinstrument vor, dass der Auftragsverarbeiter

> *„die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen [...] verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;“.*[389]

Damit ist der Auftragsverarbeiter grundsätzlich vom Verantwortlichen weisungsabhängig bzw. ihm gegenüber weisungsgebunden. Diese Weisungsgebundenheit wird für den Auftragsverarbeiter sowie für die dem

[385] Beispielhaft: Art. 58 der ETIAS-Verordnung (VO (EU) 2018/1240).

[386] Ausführlich: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 100 ff.

[387] Dazu: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 114.

[388] Dazu: Kapitel 2 D. Mittel.

[389] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 116 ff.

Verantwortlichen und dem Auftragsverarbeiter unterstellten Personen – sofern diese Zugang zu personenbezogenen Daten haben – noch einmal separat in Art. 29[390] DSGVO betont. Auch die dort genannten Akteure dürfen die „[...] Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind." Im Vergleich zum Verantwortlichen ist der Spielraum des Auftragsverarbeiters also doppelt eingeschränkt.[391] Zum einen ist dies formell durch das Weisungsrecht des Auftraggebers, also eines Verantwortlichen, bedingt. Zum anderen betrifft dies auch die inhaltliche Ebene der Verarbeitung anhand der Festlegungen des Auftraggebers. Anhand dieser Einschränkungen wird deutlich, dass beim Auftragsverarbeiter im Gegensatz zu gemeinsam Verantwortlichen gerade kein Entscheiden gemeinsam mit anderen vorliegt, sondern eines in Abhängigkeit von und im Rahmen der Vorgaben eines Verantwortlichen.

Die Weisungsgebundenheit wird zusätzlich ergänzt durch eine Verpflichtung zur Vertraulichkeit bzw. einer gesetzlichen Verschwiegenheitspflicht der zur Verarbeitung befugten Personen nach Art. 28 Abs. 3 lit. b DSGVO. Daneben besteht gem. Art. 28 Abs. 3 lit. g DSGVO nach Abschluss der Erbringung der Verarbeitungsleistungen grundsätzlich[392] eine Pflicht zur Rückgabe bzw. Löschung aller personenbezogenen Daten.[393] Zuletzt gilt ein Auftragsverarbeiter gem. Art. 28 Abs. 10 DSGVO dann als Verantwortlicher, wenn er die Zwecke und Mittel der Verarbeitung selbst bestimmt.[394] Ist der vermeintliche Auftragsverarbeiter daher entweder tatsächlich nicht weisungsgebunden oder entscheidet er über Zwecke und (wesentliche Elemente der) Mittel, so ist er selbst Verantwortlicher[395] und potenziell auch gemeinsam Verantwortlicher.

Maßgeblich für eine Auftragsverarbeitung sind nach dem Wortlaut der DSGVO also zwei Voraussetzungen: Zum einen die Weisungsgebundenheit[396] nach Art. 28

---

[390] Vgl. zu Art. 6 Abs. 5 ePrivacy-RL EuGH, Urteil vom 22.11.2012 – C-119/12 (Probst) = K&R 2013, 31, Rn. 30: „[...] auf Weisung des Diensteanbieters handelt, wenn er für die Verarbeitung von Verkehrsdaten nur auf Anweisung dieses Diensteanbieters und unter dessen Kontrolle handelt."

[391] So a.: *Kremer*, CR 2019, 225, Rn. 23.

[392] Es sei denn, es besteht eine Pflicht zur Speicherung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten.

[393] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 139 ff.

[394] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[395] *Kremer*, CR 2019, 225, Rn. 24.

[396] Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 13; Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 12; Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 66 ff.; Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 249; Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 3; S/J/T/K/*Schwartmann/Mühlenbeck*,

Abs. 3 lit. a und Art. 29 DSGVO, zum anderen die Beauftragung gem. Art. 4 Nr. 8 und Art. 28 Abs. 1 DSGVO.[397] Insgesamt lässt sich festhalten, dass charakteristisch für den Auftragsverarbeiter dessen Weisungsgebundenheit gegenüber dem Verantwortlichen sowie sein stark eingeschränkter Entscheidungsspielraum aufgrund von dessen Festlegungen sind.[398] Der Auftragsverarbeiter wird, wie in Art. 29 DSGVO besonders deutlich wird, aufgrund seiner engen Bindung und Einschränkungen gewissermaßen Teil des Verantwortlichen.[399] Man kann die Auftragsverarbeitung daher als Delegation von Aufgaben des Verantwortlichen an den Auftragsverarbeiter verstehen.[400] Auch wenn die operationale Kontrolle über die Verarbeitung beim Auftragsverarbeiter liegen kann, muss die rechtliche Kontrolle beim Verantwortlichen liegen.[401] Folglich kann man von einer Unterordnung des Auftragsverarbeiters gegenüber dem Verantwortlichen im Gegensatz zu einer Gleichrangigkeit des gemeinsam Verantwortlichen sprechen.[402]

II. Verständnis der Aufsichtsbehörden[403]

Nach der Art. 29-Datenschutzgruppe hing die Einordnung eines Akteurs als Auftragsverarbeiter von der Entscheidung des Verantwortlichen ab, Verarbeitungstätigkeiten ganz oder teilweise an eine externe Organisation zu delegieren.[404] Dabei sei der Auftragsverarbeiter im Gegensatz zu den dem

---

Art. 4 DSGVO, Rn. 178; BeckOK DatenschutzR[47]/*Spoerr*, Art. 28 DSGVO, Rn. 22 f.; *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 504; *Schreiber*, ZD 2019, 55, 55; *Kremer*, CR 2019, 225, Rn. 17.

[397] Vgl. Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 243.

[398] Paal/Pauly/*Ernst*, Art. 4 DSGVO, Rn. 56 bezeichnet ihn als quasi-„Marionette".

[399] Man kann den Auftragsverarbeiter aufgrund der Weisungsgebundenheit a. direkt als Teil des Verantwortlichen ansehen. Dies verwischt aber die Grenze zu den dem Verantwortlichen dauerhaft unterstellten Personen. Den Auftragsverarbeiter zeichnet gerade aus, dass er grundsätzlich, abseits des Auftrags, rechtlich selbstständig ist: *Monreal*, PinG 2017, 216, 219. Auch die Art. 29-Datenschutzgruppe betont neben der Beauftragung die rechtliche Selbstständigkeit: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 30.

[400] *Alsenoy*, CLSR[28] (2012), 25, 33.

[401] *Alsenoy*, CLSR[28] (2012), 25, 33.

[402] G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 28 f.

[403] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 30 ff.; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 73 ff.; *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 15 ff.

[404] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 30.

Verantwortlichen unterstellten Personen „eine rechtlich selbstständige Person, die in seinem Auftrag handelt."[405] Damit ein Akteur als Auftragsverarbeiter eingestuft werden könne, müssten zwei grundlegende Bedingungen erfüllt sein: Die fragliche Stelle[406] müsse rechtlich eigenständig sein[407] und personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Rolle des Auftragsverarbeiters ergebe sich zudem nicht ganz allgemein als eine Stelle, die Daten verarbeite, sondern aus den konkreten Tätigkeiten in einem spezifischen Kontext. Somit hänge die Einordnung als Auftragsverarbeiter oder aber Verantwortlicher immer von dem konkreten Verarbeitungsvorgang ab und könne auch dynamisch zwischen verschiedenen Vorgängen variieren. Die Art. 29-Datenschutzgruppe hob besonders das Kriterium des „im Auftrag des Verantwortlichen"-Handelns bei ihrer Analyse hervor.[408] Dies bedeute, im Interesse des Verantwortlichen zu handeln und erinnere an die Rechtsfigur der Aufgabenübertragung („Delegation").[409] Dabei solle der Auftragsverarbeiter die Weisungen des Verantwortlichen zumindest im Hinblick auf die Zwecke und die wesentlichen Elemente der Mittel befolgen. Die Rechtmäßigkeit der Verarbeitung des Auftragsverarbeiters bestimme sich durch den vom Verantwortlichen erteilten Auftrag.

Ein Auftragsverarbeiter, der den Rahmen der ihm übertragenen Aufgaben überschreite und „eine nennenswerte Rolle" bei der Entscheidung über Zwecke und wesentliche Mittel der Verarbeitung übernehme, sei (gemeinsam) Verantwortlicher.[410] Ungeachtet dieser Grenze könne der Auftragsverarbeiter trotzdem einen gewissen Ermessensspielraum in der Wahl der technischen und organisatorischen Mittel, mit denen er die Interessen des Verantwortlichen am besten wahrnehmen kann, besitzen.[411] Der Verantwortliche müsse also nicht alle Details der für die vorgesehenen Zwecke eingesetzten Mittel festlegen und billigen. Es sei jedoch erforderlich, dass er zumindest

[405] BT-Drs. 12/8329, S. 14.

[406] Das WP 169 verwendet den Wortlaut „Organisation".

[407] Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 77.

[408] Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 80.

[409] Detailliert: *Alsenoy*, CLSR[28] (2012), 25, 32 f.; *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 52.

[410] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess. Dies ist mittlerweile auch in Art. 28 Abs. 10 DSGVO normiert. Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 81.

[411] Dazu: Kapitel 2 G. III. Entscheidungsautonomie über die Mittel?

über die wichtigsten Elemente[412] der Verarbeitungsstruktur informiert werde.[413] Andererseits könne der Auftragsverarbeiter gegenüber dem Verantwortlichen auch Vorschläge bezüglich der wesentlichen Elemente der Mittel machen, solange der Verantwortliche hierüber selbst entscheide.[414] Schließlich sei der zwischen dem Verantwortlichen und dem Auftragsverarbeiter zu schließende Vertrag nicht konstitutiv für das Bestehen einer Auftragsverarbeitung, sondern vielmehr Folge der Entscheidung zu einer Auftragsverarbeitung.[415] Maßgeblich sei damit ein funktioneller Ansatz bei der Feststellung einer Auftragsverarbeitung.[416] Die Auftragsverarbeitung erschließe sich aus einer Analyse der tatsächlichen Umstände, nicht der formellen.[417] Daher machen die Art. 29-Datenschutzgruppe und der EDPB die Einordnung eines Akteurs als Verantwortlicher, gemeinsam Verantwortlicher oder Auftragsverarbeiter an dessen Entscheidungsspielraum fest.[418]

Daneben finden sich im WP 169 der Art. 29-Datenschutzgruppe sowie den Leitlinien zum Verantwortlichen des EDPB auch Beispiele zur Abgrenzung von Auftragsverarbeitern und gemeinsam Verantwortlichen.

Den klassischen Fall einer Auftragsverarbeitung stellte die Art. 29-Datenschutzgruppe in WP 169 zunächst am Beispiel der Direktwerbung[419] dar. Ein Unternehmen ABC schließt Verträge mit verschiedenen Organisationen für die

---

[412] Z.B. beteiligte Akteure, Sicherheitsmaßnahmen, Gewähr hinsichtlich der Verarbeitung in Drittländern usw.

[413] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 34. Vgl. OVG Schleswig, Beschluss vom 12.01.2011 – 4 MB 56/10 = CR 2011, 359, 363.

[414] Vgl. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 16 f.

[415] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 103 Fn. 42.

[416] Vgl. zum funktionellen Konzept: Kapitel 2 E. V. Typologie anstatt formeller Analyse (Art. 29-Datenschutzgruppe / Europäischer Datenschutzausschuss).

[417] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 12.

[418] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 16; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 37 ff. Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 6 stellt die Position der Art. 29-Datenschutzgruppe zur Abgrenzung Verantwortlicher und Auftragsverarbeiter zusammengefasst dar.

[419] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17 Beispiel 2 (Direktwerbung); ähnlich a.: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40. Beispiel 1 (Gehaltsabrechnung), hier besitzt der Auftragsverarbeiter allerdings einen geringen Spielraum hinsichtlich der Mittel (etwa verwendete Software, Zugriff innerhalb des Unternehmens).

Durchführung seiner Direktwerbekampagnen einerseits sowie der Gehaltsabrechnung andererseits ab. ABC gibt klare Weisungen an die Organisationen.[420] Obwohl die Organisationen eine gewisse Ermessensfreiheit haben,[421] sind ihre Aufgaben recht klar und eng festgelegt. Der Werbeversender kann zwar Empfehlungen an ABC geben, ist jedoch an die Weisungen von ABC gebunden. Darüber hinaus ist nur eine Organisation, ABC selbst, dazu berechtigt, die verarbeiteten Daten zu nutzen. Alle anderen Organisationen müssen darauf vertrauen, dass ABC auf einer rechtlichen Grundlage handelt, sollte ihr Recht, die Daten zu verarbeiten, in Frage gestellt werden. In diesem Beispiel handele es sich bei dem Unternehmen ABC klar um den Verantwortlichen, während die anderen Organisationen Auftragsverarbeiter von ABC seien. Sofern die Organisation, die mit der Gehaltsabrechnung betreut ist, für die Auszahlung des Gehalts zudem Daten an eine Bank übermittele, handele es sich bei dieser Verarbeitung allerdings nicht um eine zusätzliche Auftragsverarbeitung der Bank für ABC, sondern eine Übermittlung der Daten von ABC an die Bank.[422] Denn die Bank entscheide selbst über die Zwecke und Mittel der Verarbeitung der übermittelten Daten.

Als weiteres Beispiel zur Veranschaulichung des Konzeptes des Auftragsverarbeiters verwendete die Art. 29-Datenschutzgruppe in WP 169 einen Host-Providers.[423] Solange dieser Provider die von seinen Kunden auf einer Website veröffentlichten Daten nicht für eigene Zwecke weiterverarbeite,[424] liege grundsätzlich eine Auftragsverarbeitung gegenüber den Kunden vor.[425] Auch der EDPB erachtet in seinen Leitlinien einen Host-Provider, der verschlüsselte Daten seiner Kunden speichert, als Auftragsverarbeiter.[426] Dieser Host-Provider entscheide nicht darüber, ob die Daten Personenbezug aufweisen, noch fände eine weitere Verarbeitung abseits der Speicherung statt. Daneben versteht der EDPB in seinen Leitlinien auch die Gehaltsabrechnung über eine externe Stelle als Auftragsverarbeitung, sofern diese Stelle

[420] Welches Werbematerial zu versenden ist und an wen; welche Beträge bis zu welchem Datum an wen zu zahlen sind usw.

[421] Einschließlich der Wahl der eingesetzten Software.

[422] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40 Beispiel 2 Bankzahlungen.

[423] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 31. Ähnlich: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40 Beispiel 4 Host-Provider.

[424] Vgl. *Kremer*, CR 2019, 225, Rn. 28 f. zu SaaS.

[425] Vgl. a. *Kremer*, CR 2019, 225, Rn. 27.

[426] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40 Beispiel 4 Host-Provider.

die Daten nicht für eigene Zwecke verwendet und klare Weisungen des Verantwortlichen erhält.[427]

Wie das Beispiel 21[428] der Art. 29-Datenschutzgruppe in WP 169 zeigte, stellen aber bestimmte Berufsstände aufgrund ihrer berufsrechtlichen Regelungen, trotz auftragsverarbeitungsähnlicher Sachlage, Verantwortliche dar.[429] Explizit erwähnt wurden dabei nur Rechtsanwälte, Rechnungsprüfer und Steuerberater. Die Einordnung als Verantwortliche könne allerdings bei Rechnungsprüfern und Steuerberatern aufgrund von gesetzlichen Verpflichtungen einerseits sowie engen Aufträgen/Weisungen durch den Auftraggeber andererseits durchaus variieren, wie Beispiel 23[430] illustrierte.[431] Soweit Rechnungsprüfer und Steuerberater Dienstleistungen auf Grundlage sehr allgemeiner Weisungen erbringen („Erstellen Sie meine Steuererklärung"), seien sie Verantwortliche. Wenn ein Rechnungsprüfer jedoch für ein Unternehmen tätig werde, beispielsweise um eine umfassende Buchprüfung vorzunehmen, und dabei ausführlichen Weisungen des fest angestellten Buchprüfers des Unternehmens unterliege, dann sei er aufgrund der klaren Weisungen und des mithin eingeschränkten Handlungsspielraums generell als Auftragsverarbeiter einzustufen. Soweit ein Rechnungsprüfer dabei allerdings wiederum ein meldepflichtiges Fehlverhalten feststelle, handele er aufgrund seiner beruflichen Verpflichtung als ein Verantwortlicher.

Ein weiteres variables Szenario fand sich in Beispiel 25 des WP 169 der Art. 29-Datenschutzgruppe.[432] In diesem Beispiel beauftragt ein Pharmaunternehmen mehrere Studienzentren mit Arzneimittelstudien. Je nach konkreter Ausgestaltung könnten die Studienzentren zusammen mit dem Pharmaunternehmen gemeinsam Verantwortliche darstellen.[433] Diese Einordnung solle vor allem von der Autonomie der Studienzentren abhängen. In dem konkreten Beispiel scheint dies mit der Information der betroffenen

[427] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40 Beispiel 1 Gehaltsabrechnung.

[428] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 35.

[429] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 35.

[430] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 35.

[431] Ebenso: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40 Beispiel 3 Buchhalter.

[432] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 36 f.

[433] *Kremer*, CR 2019, 225, Rn. 19 f. vergleicht dies mit der gemeinsamen Infrastruktur in Unternehmensgruppen. Je nach Entscheidungsautonomie der Beteiligten kann eine gemeinsame Verantwortlichkeit, Auftragsverarbeitung oder alleinige Verantwortlichkeit vorliegen.

Personen sowie der Einholung der Einwilligung zusammenzuhängen. Daneben seien die Studienzentren auch für die Sicherheit der Unterlagen bzw. personenbezogenen Daten verantwortlich. Dass es sich um eine gemeinsame Verantwortlichkeit und nicht um eine reine Übermittlung handelt, scheint durch den Zweck der Durchführung klinischer Studien als Vorgangsreihe bedingt. Dabei sollen sowohl Pharmaunternehmen als auch Studienzentren wichtige Entscheidungen über das „Wie" der Verarbeitung treffen. Lege das Pharmaunternehmen als Auftraggeber hingegen die Zwecke und wesentlichen Elemente der Mittel der Verarbeitung fest und verbleibt den Studienzentren nur ein sehr enger Handlungsspielraum, könnte es sich um eine Auftragsverarbeitung handeln.

III. Entscheidungsautonomie über die Mittel?

Hinsichtlich der Abgrenzung zu gemeinsam Verantwortlichen stellt sich bei dem Auftragsverarbeiter die Frage, inwieweit dieser zumindest teilweise eigene Entscheidungen treffen kann. Trotz seiner allgemeinen Weisungsgebundenheit verbleibt dem Auftragsverarbeiter grundsätzlich, wie bereits dargestellt, eine gewisse Entscheidungsautonomie.[434] Dabei ist allerdings strittig, wie weit diese reicht.[435] So ist nach dem EDPB nur ein solches Szenario klar als Auftragsverarbeitung zu erachten, in dem der Verantwortliche über die Zwecke und Mittel der Verarbeitung entscheidet und dem Auftragsverarbeiter nur die Ausführung seiner spezifischen Anweisungen überlässt.[436] Aus Art. 28 Abs. 3 lit. c DSGVO wird deutlich, dass der Auftragsverarbeiter jedenfalls die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung trifft.[437] Mindestens so weit reicht also seine Entscheidungsautonomie.[438]

Ob diese noch weiter reicht, hängt davon ab, wie man den Begriff der Mittel der Verarbeitung versteht. Nach dem Verständnis der Art. 29-Datenschutzgruppe und des EDPB beinhalten die Mittel sowohl wesentliche Elemente wie auch unwesentliche Elemente.[439] Die wesentlichen Elemente der Mittel sollen die verarbeiteten

[434] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 37.

[435] Kritisch im Hinblick auf die Mittel: Ehmann/Selmayr/*Klabunde/Horvath*, Art. 4 DS-GVO, Rn. 41. Großzügig: G/S/S/V/*Kramer*, Art. 28 DSGVO, Rn. 98 ff.

[436] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 38.

[437] So wohl a.: G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40.

[438] Zutreffend insoweit: *Kremer*, CR 2019, 225, Rn. 25.

[439] Dazu: Kapitel 2 D. Mittel.

personenbezogenen Daten selbst sowie Entscheidungen über diese betreffen, etwa die Speicherdauer.[440] Die unwesentlichen Elemente hingegen sollen technische und organisatorische Fragen betreffen, so etwa die verwendete Soft- und Hardware.[441] Allerdings ist es gerade bei standardisierter Soft- oder Hardware vorstellbar, dass deren Auswahl eine Rückwirkung auf die wesentlichen Elemente der Mittel, also etwa die verarbeiteten personenbezogenen Daten, hat.[442] Denkbar ist etwa, dass die Verwendung einer bestimmten Software nur mit dem Zugriff Dritter auf die verarbeiteten personenbezogenen Daten erfolgen kann.

Nach Ansicht der Art. 29-Datenschutzgruppe kann ein Auftragsverarbeiter über die technischen und organisatorischen Mittel selbst entscheiden, eine Entscheidung über die wesentlichen Elemente der Mittel hingegen impliziere eine Verantwortlichkeit.[443] Diese wesentlichen Elemente der Mittel lassen sich vor allem in der Festlegung durch den Verantwortlichen in Art. 28 Abs. 3 DSGVO erkennen.[444] Vor diesem Hintergrund ist die Frage, ob der Auftragsverarbeiter insgesamt über die Mittel der Verarbeitung autonom entscheiden kann, zu verneinen.[445] Unschädlich ist allerdings eine Beratung des Verantwortlichen bezüglich der wesentlichen Elemente der Mittel, sofern der Verantwortliche letztlich selbst entscheidet.[446] Bei den unwesentlichen Elementen der Mittel wiederum ist zu hinterfragen, ob eine Entscheidung hierüber nicht indirekt die wesentlichen Elemente der Mittel berührt.

IV. Das Eigeninteresse als eigener Zweck?

Der EuGH erwähnt in seiner Rechtsprechung zur gemeinsamen Verantwortlichkeit mittlerweile mit einer gewissen Regelmäßigkeit das Eigeninteresse[447] eines

[440] So a.: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 67.

[441] Dies spiegelt sich a. im ursprünglichen Entwurf der Kommission (BR-Drs. 690/90, S. 52 f.) in der Aufteilung der Mittel in Art der Daten, Verarbeitungsverfahren und Zugang Dritter zu den Daten wider. In diesem Sinne könnte der Auftragsverarbeiter also nur über das Verarbeitungsverfahren autonom entscheiden. Ebenso: *Mester/Öztürk*, DuD 2023, 73, 75.

[442] Unklar insoweit hinsichtlich der technischen und organisatorischen Maßnahmen: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 41 mit Beispiel.

[443] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[444] Vgl. Paal/Pauly/*Martini*, Art. 28 DSGVO, Rn. 36.

[445] Anders: *Kremer*, CR 2019, 225, Rn. 25.

[446] *Cimina*, ERA Forum 2020, 5.

[447] Dieses ist wiederum vom „(wirtschaftlichen) Interesse“ in EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80 abzugrenzen. Das Eigeninteresse betrifft die Frage der Entscheidungsautonomie, während das „(wirtschaftliche) Interesse“ eine Frage der Zweckkomplementarität zwischen den gemeinsam Verantwortlichen ist. Dazu: Kapitel 4 E. I. 6. „Interesse“ als

Verantwortlichen.[448] Der Begriff fällt dabei nur im Zusammenhang mit gemeinsam Verantwortlichen bzw. in Szenarien mit mehreren Akteuren. So sei ein Akteur dann gemeinsam Verantwortlicher, wenn er aus Eigeninteresse Einfluss auf die Verarbeitung nehme.

Denkbar ist es also, für eine Abgrenzung zwischen Auftragsverarbeiter und gemeinsam Verantwortlichen darauf abzustellen, ob und welches Eigeninteresse ein Akteur mit einer Verarbeitung verfolgt.[449] Stellt man das Eigeninteresse mit einem eigenen Zweck gleich, sollte ein Auftragsverarbeiter grundsätzlich kein Eigeninteresse an einem Verarbeitungsvorgang als solchem haben.[450] Denn aus Art. 28 Abs. 10 DSGVO ergibt sich, dass ein Auftragsverarbeiter, der über die Zwecke und Mittel der Verarbeitung entscheidet, als Verantwortlicher angesehen wird.[451] Sofern also das Eigeninteresse mit einem eigenen Zweck gleichzusetzen ist, wäre ein vermeintlicher Auftragsverarbeiter mit Eigeninteresse tatsächlich ein Verantwortlicher.[452]

Dabei hat ein Auftragsverarbeiter natürlich ein Eigeninteresse an einer Verarbeitung dahingehend, dass er aufgrund der Durchführung der Verarbeitung üblicherweise eine Vergütung erhält.[453] Darüber hinaus hat ein Auftragsverarbeiter an der Verarbeitung selbst aber üblicherweise kein Interesse.[454] Ein Auftragsverarbeiter, dessen einziges Interesse die Entlohnung ist, bewegt sich daher grundsätzlich nur im Rahmen des Spielraums, der ihm aufgrund der Weisungsgebundenheit gegenüber dem Verantwortlichen verbleibt. Denkbar sind allerdings auch Fälle, in denen der Auftragsverarbeiter statt oder neben einer monetären Vergütung Ergebnisse der Verarbeitung selbst oder in deren Rahmen erhobene personenbezogene Daten als Vergütung erhalten könnte. Damit würde der Auftragsverarbeiter also über die monetäre Vergütung hinaus ein Eigeninteresse an der Verarbeitung selbst verfolgen.[455]

Zweckkomplementarität.

[448] Zuerst in EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 68, dann EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 68.

[449] *Hanloser*, ZD 2019, 455, 459; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 12.

[450] G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40.

[451] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[452] Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 145 ff.

[453] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 62; *Lezzi/Oberlin*, ZD 2018, 398, 400.

[454] So sprechen *Mester/Öztürk*, DuD 2023, 73, 75 davon, dass der Auftragsverarbeiter kein vorrangig eigenes Interesses an der Verarbeitung hat. Daher dürfte bei *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23 Beispiel 6 allein die Gewinnmaximierung von H unbeachtlich sein.

[455] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23 Beispiel 6. Dies scheint *Hanloser*, ZD 2019, 455, 459 zu übersehen.

Insofern entscheidet der Auftragsverarbeiter notwendigerweise auch über seinen eigenen Zweck. Diesen eigenen Zweck muss er dann allerdings auch im Rahmen dieses konkreten Verarbeitungsvorgangs bzw. dieser Vorgangsreihe verfolgen können.[456] Trotz eines Eigeninteresses oder eigenen Zweckes scheint es daher plausibel, dass ein Auftragsverarbeiter in solchen Szenarien dennoch innerhalb des Spielraums seiner Weisungsgebundenheit bleibt.[457] Der Auftragsverarbeiter würde dann zwar keine eigenen Zwecke im Rahmen der Auftragsverarbeitung selbst verfolgen, aber aufgrund der Ergebnisse der Verarbeitung oder der erhobenen Daten nach Beendigung der Auftragsverarbeitung weitere, eigene Verarbeitungen durchführen. So hätte der vermeintliche Auftragsverarbeiter also zwar ein Eigeninteresse an der fraglichen Verarbeitung als notwendigem Zwischenschritt zur Erlangung der Daten, er würde allerdings in dieser selbst noch keine eigenen Zwecke verfolgen. Aufgrund dieser Erwägungen ist es schwierig, ein Eigeninteresse des Auftragsverarbeiters allgemein mit eigenen Zwecken gleichzusetzen.

Legt ein Auftragsverarbeiter hingegen aufgrund von Eigeninteresse eigene Zwecke nicht nur im Rahmen eines nachgelagerten, unabhängigen Verarbeitungsvorgangs fest,[458] sondern bereits im Rahmen der der vermeintlichen Auftragsverarbeitung unterfallenden Verarbeitungsvorgänge, so ist er gem. Art. 28 Abs. 10 DSGVO bereits für diese Vorgänge Verantwortlicher.[459] Es handelt sich dann um einen „rogue processor". Nutzt der vermeintliche Auftragsverarbeiter etwa Daten, die er im Rahmen einer Auftragsverarbeitung erhält, ohne die Genehmigung des Verantwortlichen um seine eigene Datenbank zur ergänzen, verfolgt er neben der eigentlichen Auftragsverarbeitung noch andere, eigene Zwecke. Eine nachgelagerte Verarbeitung liegt etwa auch dann regelmäßig[460] vor, wenn der vorherige Auftragsverarbeiter im Rahmen einer Forderungsabtretung die Forderung im eigenen Namen geltend macht.[461] Die dazu erforderliche Übermittlung der notwendigen personenbezogenen

[456] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 28 f.

[457] A.A. anscheinend: *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 45; Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 251.

[458] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18: „[...] für eine andere Verarbeitungstätigkeit [...]".

[459] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18; ähnlich wohl a.: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 28 f.

[460] Eine Ausnahme kann theoretisch aufgrund spezifischer schuldrechtlicher Vereinbarungen vorliegen.

[461] VG Mainz, Urteil vom 20.02.2020 – 1 K 467/19.MZ, Rn. 22 ff.; VG Wiesbaden, Beschluss vom 13.05.2024 – 6 K 11306/22.WI = BeckRS 2024, 11305.

Daten ist nicht mehr von der Auftragsverarbeitung privilegiert[462] und stellt auch keine gemeinsame Verantwortlichkeit dar, da der ursprünglich Verantwortliche mit der Forderungsabtretung keinen eigenen Zweck mehr verfolgt. Sie stellt vielmehr eine reine Übermittlung zwischen singulären Verantwortlichen dar, die einer Verarbeitungsrechtfertigung bedarf, etwa Art. 6 Abs. 1 lit. b DSGVO.[463]

Sinnvoll anzuwenden ist das Eigeninteresse daher als Indiz für die Verfolgung eigener Zwecke innerhalb eines konkreten Verarbeitungsvorgang. Allerdings muss es dabei immer daraufhin überprüft werden, ob es sich nicht um ein im Rahmen der Auftragsverarbeitung vertretbares Eigeninteresse handelt. Zu beachten ist auch, dass das Eigeninteresse in der Rechtsprechung des EuGH immer mit der Einflussnahme auf eine Verarbeitung gekoppelt und somit vor allem als Abgrenzungselement zur Weisungsgebundenheit zu verstehen ist.[464]

Denkbar, wenn auch eher unwahrscheinlich, ist das Szenario, dass ein Akteur aus altruistischem Interesse eine Verarbeitung unterstützt. In diesem Szenario würde gerade kein Eigeninteresse vorliegen. Entscheidendes Abgrenzungskriterium zwischen dem Verantwortlichen und dem Auftragsverarbeiter ist neben dem Eigeninteresse aber vor allem die Weisungsgebundenheit. Daher wäre zunächst zu prüfen, inwiefern ein koordiniertes Vorgehen zwischen dem Verantwortlichen und dem unterstützenden Akteur besteht. Sofern der Unterstützer bereit ist, sich den Weisungen des Verantwortlichen zu unterwerfen, könnte es sich um eine Auftragsverarbeitung handeln. Andernfalls wäre, sofern die Unterstützung nicht erkennbar gegen den Willen des Verantwortlichen erfolgt, eine gemeinsame Verantwortlichkeit anzunehmen. Es erscheint unbillig, dem Verantwortlichen eine gemeinsame Verantwortlichkeit gegen seinen Willen aufzuzwingen. Maßgeblich für die Vermutung dieses Willens und somit einer gemeinsamen Verantwortlichkeit dürfte eine Zweckkomplementarität sein, also die Frage, ob die Verarbeitung auch im Interesse des (unterstützten) Verantwortlichen erfolgt.[465] Daneben wären allerdings auch entsprechende technische und organisatorische Maßnahmen zu berücksichtigen, die einen Einfluss des Unterstützers auf die Verarbeitung verhindern könnten. Möglich erscheint eine gemeinsame Verantwortlichkeit des Verantwortlichen mit dem Unterstützer also auch dann, wenn

[462] Dies würde eine Umgehung von Art. 6 Abs. 1 DSGVO bedeuten.

[463] Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 92 mit Beispiel.

[464] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 68: „[...] aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt [...]".

[465] Dazu: Kapitel 4 E. I. 6. „Interesse" als Zweckkomplementarität. Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

nur eine Zweckkomplementarität zwischen dem Unterstützer und dem Verantwortlichen vorliegt und die Verarbeitung weder technisch oder organisatorisch abgesichert ist.[466] Solange allerdings nur eine nicht erbetene Übermittlung von Daten vom Unterstützer zum Verantwortlichen vorliegt, handelt es sich nicht um gemeinsam Verantwortliche, sondern jeweils singuläre Verantwortliche.[467]

[466] Vgl. *Roßnagel*, MMR 2005, 71, 74: „[...] - vielleicht nicht intendierten - Zusammenwirkens [...]" Dabei stellt sich die Folgefrage, welche Mindestpflichten bei einer solchen ungewollten gemeinsamen Verantwortlichkeit bestehen: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 29.

[467] Sofern der Empfänger der Daten diese überhaupt weiterverarbeitet.

Kapitel 3

Folgen der Verantwortlichkeit

Schwerpunkt dieser Arbeit sind die Voraussetzungen einer datenschutzrechtlichen Verantwortlichkeit. Da aber hinsichtlich der Voraussetzungen auch eine systematische Wechselwirkung zu den Folgen der Verantwortlichkeit besteht, müssen auch die Folgen der Verantwortlichkeit untersucht werden. Ausgeklammert werden sollen hierbei weitestgehend die unmittelbaren Folgen der Verantwortlichkeit im Sinne der Verhaltenspflichten. Der Fokus dieses Teils liegt daher auf den Sekundärfolgen der Verantwortlichkeit. Zu den wichtigsten Sekundärfolgen der Verantwortlichkeit gehört die Haftung auf Schadensersatz nach Art. 82 DSGVO. In diesem Zusammenhang ist das Verhältnis der DSGVO zum Digital Services Act (DSA) maßgeblich. Daneben sind die Geldbußen gem. Art. 83 DSGVO eine gleichermaßen bedeutende Sekundärfolge. Spezifische Folgen der gemeinsamen Verantwortlichkeit werden im Zusammenhang mit der gemeinsamen Verantwortlichkeit insgesamt behandelt.[1]

A. Haftung auf Schadensersatz

Nähere Details zur Haftung als eigenständigem Konzept neben der Verantwortlichkeit finden sich in der DSGVO kaum.[2] Der Begriff Haftung findet vor allem im Zusammenhang mit dem Schadenersatz in Art. 82 DSGVO Erwähnung. Art. 82 Abs. 1 DSGVO formuliert den Grundsatz, dass der Verantwortliche oder Auftragsverarbeiter für materielle oder immaterielle Schäden aufgrund eines Verstoßes gegen die DSGVO haftet. Dabei haftet gem. Art. 82 Abs. 2 S. 1 DSGVO jeder an einer Verarbeitung beteiligte Verantwortliche.[3] Eine gemeinsame Verantwortlichkeit zwischen den Beteiligten wird gerade nicht vorausgesetzt. Der Auftragsverarbeiter hingegen haftet nur eingeschränkt nach Art. 82 Abs. 2 S. 2 DSGVO. Neben der Haftung des Auftragsverarbeiters gem. Art. 82 Abs. 2 S. 2 DSGVO stellt aber Art. 28 Abs. 10

[1] Dazu: Kapitel 4 L. Folgen der gemeinsamen Verantwortlichkeit.

[2] Zum Verhältnis der Begriffe Verantwortlichkeit und Haftung in Art. 26 DSGVO: Kapitel 4 L. III. Art. 26 Abs. 3 DSGVO als „gesamtschuldnerische Verantwortlichkeit"?

[3] Kühling/Buchner/*Bergt*, Art. 82 DS-GVO, Rn. 22.

DSGVO klar, dass im Falle eines Auftragsverarbeiterexzesses[4] eine Haftung des ursprünglichen Verantwortlichen sowie eine Sanktionsmöglichkeit gegenüber dem ursprünglich Verantwortlichen bestehen bleibt.[5] Sofern eine Haftung nach Art. 82 Abs. 2 DSGVO von mehreren Verantwortlichen und/oder Auftragsverarbeitern für dieselbe Verarbeitung gegeben ist, haften diese zudem gesamtschuldnerisch gem. Art. 82 Abs. 4 DSGVO.[6] Leistet ein Verantwortlicher oder Auftragsverarbeiter gem. Art. 82 Abs. 4 DSGVO Schadensersatz, kann dieser gem. Art. 82 Abs. 5 DSGVO bei den übrigen an derselben Verarbeitung Beteiligten Regress nehmen. Der Anteil des Regresses soll dabei dem Teil entsprechen, der unter den in Art. 82 Abs. 2 DSGVO festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht. Dies ist also so zu verstehen, dass gem. Art. 82 Abs. 5 DSGVO der jeweilige Verantwortungsbeitrag maßgeblich für die Regresshaftung ist.[7] Dieser kann in der umfassenden Verantwortung für einen Verarbeitungsvorgang aus mehreren bestehen, ebenso aber auch im anteiligen Verantwortungsbeitrag für einen einzelnen Vorgang. Nicht hinreichend eindeutig ist allerdings die Berechnung des Verantwortungsbeitrags.[8] Abseits einer Regelung der internen Verantwortlichkeit für die Erfüllung der verletzten Pflichten oder Betroffenenrechte im Rahmen von Art. 26 Abs. 1 DSGVO oder Art. 28 Abs. 3 DSGVO, scheint es angemessen, den gesamtschuldnerisch Haftenden eine Haftung zu gleichen Anteilen zuzumuten. In diesem Zusammenhang ist auch die Entlastungsmöglichkeit nach Art. 82 Abs. 3 DSGVO sinnvoll.

I. Rechtsprechung des EuGH

Unabhängig von der Haftung aus Art. 82 DSGVO hatte der EuGH in der Rechtssache Fashion ID[9] die Haftung eines gemeinsam Verantwortlichen für der gemeinsamen Verantwortlichkeit vor- oder nachgelagerte Verarbeitungsvorgänge[10] auf zivilrechtlicher Basis nach mitgliedstaatlichem Recht nicht ausgeschlossen.[11] Folglich

[4] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[5] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 56.

[6] Kritisch zu den Besonderheiten für den Auftragsverarbeiter: Ehmann/Selmayr/*Nemitz*, Art. 82 DS-GVO, Rn. 55 ff.

[7] Taeger/Gabel/*Moos/Schefzig*, Art. 82 DSGVO, Rn. 131; Ehmann/Selmayr/*Nemitz*, Art. 82 DS-GVO, Rn. 64.

[8] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[9] Dazu: Kapitel 4 B. III. Fashion ID.

[10] Also solche Vorgänge für die keine gemeinsame Verantwortlichkeit mehr besteht.

[11] Dazu: Kapitel 5 J. Störerhaftung und Zweckveranlasser. EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74.

regelt die DSGVO, jedenfalls nach der Auslegung des EuGH, eine solche Haftung nicht abschließend. Da den von dieser Haftung betroffenen Akteur aber gar keine Verantwortlichkeit für die maßgeblichen vor- oder nachgelagerten Verarbeitungsvorgänge trifft, kann die Haftung der DSGVO auch mangels Verantwortlichkeit gar nicht abschließend sein.

II. Verständnis der Aufsichtsbehörden

Hinsichtlich der zivilrechtlichen Haftung erkannte die Art. 29-Datenschutzgruppe keine besonderen Probleme beim Verantwortlichen.[12] So könnten aus demselben Lebenssachverhalt unterschiedliche Stellen zivilrechtlich haften. Dies wird in Beispiel 4 des WP 169 veranschaulicht. In diesem Beispiel haften sowohl ein Unternehmen aufgrund unzureichender Sicherheitsmaßnahmen als auch ein Vorstandsmitglied für die unrechtmäßige Nutzung von Daten aus einer heimlichen Mitarbeiterüberwachung.[13] Dabei bestehe die jeweilige Haftung unabhängig von einer gemeinsamen Verantwortlichkeit oder einer Auftragsverarbeitung.

Im Hinblick auf die DSRL stellte sich, ohne eine Art. 82 Abs. 4 DSGVO entsprechende Regelung, zudem die Frage, ob eine gemeinsame Verantwortlichkeit stets eine gesamtschuldnerische Haftung bedinge.[14] Dies lehnte die Art. 29-Datenschutzgruppe ab. Es gebe eine Unzahl denkbarer Verarbeitungsszenarien, daher sei eine pauschale Gesamtschuld nicht angebracht. Durch die klare, interne Zuweisung von Pflichten und den entsprechenden Informationen gegenüber den betroffenen Personen sollten „negative Kompetenzkonflikte“ vermieden werden. Lasse sich eine solche Transparenz nicht herstellen, insbesondere bei einer Vielzahl von beteiligten Akteuren, solle allein aufgrund der Verletzung des Grundsatzes der Verarbeitung nach Treu und Glauben eine Gesamtschuld angenommen werden können.[15]

Zudem hatte die Art. 29-Datenschutzgruppe in WP 169 angedeutet, dass nach mitgliedstaatlichem Recht eine strafrechtliche oder verwaltungsrechtliche Haftung

[12] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20.

[13] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 21.

[14] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 27.

[15] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 29 f.

auch für jede andere Person neben dem Verantwortlichen, die gegen das Datenschutzrecht verstoße, denkbar sei.[16]

B. Das Verhältnis von DSGVO und e-Commerce-RL bzw. DSA[17]

Unklar ist im Zusammenhang mit der Haftung des Verantwortlichen vor allem auch das Verhältnis der DSGVO zum DSA.[18] Beide Gesetzeswerke nehmen sich gegenseitig in Bezug. So sieht die DSGVO in Art. 2 Abs. 4 vor:

> *„Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.“*[19]

Art. 2 Abs. 4 lit. g DSA wiederum sieht vor:

> *„Diese Verordnung lässt die Vorschriften anderer Rechtsakte der Union unberührt, die andere Aspekte der Erbringung von Vermittlungsdiensten im Binnenmarkt regeln oder diese Verordnung präzisieren und ergänzen, insbesondere folgende: [...] g) die Unionsvorschriften zum Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG [...]“*[20].

Über die Verweisungsnorm des Art. 89 Abs. 2 DSA gilt Art. 2 Abs. 4 DSGVO entsprechend für die Art. 4, 5, 6 und 8 DSA. Kernproblem dieser beidseitigen „lässt die Anwendung unberührt“-Regelung ist nun deren Reichweite. Denkbar ist zunächst,

---

[16] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20 Fn. 15.

[17] In der begutachteten Version dieser Arbeit wurde noch die e-Commerce-RL behandelt. Zwischenzeitlich wurden durch Art. 89 Abs. 1 DSA die Art. 12-15 e-Commerce-RL gestrichen. Maßgeblich sind nun gem. Art. 89 Abs. 2 DSA die Art. 4, 5, 6 und 8 DSA. Die notwendigen Anpassungen wurden zwar vorgenommen, allerdings beziehen sich weite Teile der Literatur noch auf die e-Commerce-RL.

[18] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste).

[19] Dazu: ErwGr 21 DSGVO.

[20] Dazu: ErwGr 10 DSA.

dass beide Gesetzeswerke in ihrem Regelungsbereich abschließend sind.[21] Der DSA hätte also hinsichtlich der Haftung im Bereich der DSGVO keine Konsequenz, die DSGVO wiederum im Anwendungsbereich der DSA, abseits einer expliziten Anordnung, keine Auswirkung. Daneben ist aber auch denkbar, dass der DSA die Haftung nach Art. 82 DSGVO für Schadensersatz modifiziert. Denkbar ist diese Modifikation insbesondere aufgrund der Haftungsprivilegierungen des DSA nach Art. 4 ff., die Art. 2 Abs. 4 DSGVO explizit erwähnt.

Die e-Commerce-RL sprach in den Art. 12 - 14 noch davon, dass ein Diensteanbieter nicht verantwortlich sei. Der DSA spricht in den Art. 4 - 6 nunmehr nur noch davon, dass ein Diensteanbieter nicht hafte. Demnach ist durch den DSA nunmehr keine Einschränkung der materiellrechtlichen Pflichten des Verantwortlichen gem. Art. 4 Nr. 7 DSGVO abseits der Haftung nach Art. 82 DSGVO denkbar. Einige der folgenden Überlegungen, die sich auf den Wortlaut der e-Commerce-RL beziehen, sind somit nur noch für eine Fortentwicklung des Konzeptes der datenschutzrechtlichen Verantwortlichkeit relevant.

I. Rechtslage zur DSRL

Um das Verhältnis der DSGVO zum DSA zu verstehen, muss auch das Verhältnis der DSRL zur damals noch geltenden e-Commerce-RL als jeweilige Vorgängergesetze untersucht werden. Denn die einzige Neuerung der DSGVO gegenüber der DSRL hinsichtlich dieses Verhältnisses ist Art. 2 Abs. 4 DSGVO mit dem ergänzenden ErwGr 21 DSGVO. Abseits eines abweichenden Wortlautes finden sich in Art. 2 Abs. 4 lit. g DSA und ErwGr 10 DSA keine materiellen Änderungen zum Anwendungsbereich gegenüber der e-Commerce-RL.

Die DSRL konnte sich noch nicht zur e-Commerce-RL verhalten, da die DSRL vor der e-Commerce-RL erlassen wurde. Allein aus dem Fehlen einer Art. 2 Abs. 4 DSGVO entsprechenden Regelung in der DSRL konnte also noch nichts zum Verhältnis der Richtlinien untereinander abgeleitet werden. Insoweit sich die e-Commerce-RL aber im Anwendungsbereich der DSRL selbst für unanwendbar erklärte, schien das Verhältnis der Richtlinien zueinander relativ klar. Deutlich, insbesondere im Hinblick auf die datenschutzrechtliche Verantwortlichkeit, erschien auch ErwGr 14 e-Commerce-RL[22]:

[21] So kann man etwa ErwGr 10 DSA verstehen: „Der Schutz von Einzelpersonen bei der Verarbeitung personenbezogener Daten wird einzig durch die Vorschriften des Unionsrechts in diesem Bereich geregelt, insbesondere durch die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG."

[22] Weitgehend identisch: ErwGr 10 DSA.

> *„Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ausschließlich Gegenstand der Richtlinie 95/46/EG [...]. Die Grundsätze des Schutzes personenbezogener Daten sind bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten, insbesondere in bezug [sic] auf [...] die Verantwortlichkeit von Vermittlern. [...].“*

1. Haftungsprivilegierungen als Modifikation der Haftung nach Art. 82 DSGVO?

Da aber beide Richtlinien den Begriff der Verantwortlichkeit verwendeten, war ErwGr 14 e-Commerce-RL missverständlich. So sprach die englische Version des ErwGr 14 e-Commerce-RL von „liability of intermediaries“ anstatt von „Verantwortlichkeit von Vermittlern“. Dies konnte so verstanden werden, dass Verantwortliche im Sinne der e-Commerce-RL die DSRL zu beachten hätten. Es hätte dann aber umgekehrt nichts darüber ausgesagt, ob die Privilegierungen der e-Commerce-RL für Verantwortliche im Sinne der DSRL gelten. Demnach hätten die Haftungsprivilegierungen aus Art. 12 ff. e-Commerce-RL eine Verantwortlichkeit nicht ausgeschlossen. Eine Haftungsprivilegierung nach Art. 12 ff. e-Commerce-RL für Schadensersatzforderungen wäre aber möglich geblieben. Dieses Verständnis schien auch dadurch gestützt zu werden, dass die DSGVO in der englischen Sprachfassung weiterhin begrifflich zwischen „responsibility“ in Art. 24 DSGVO und „liability“ in Art. 82 DSGVO unterscheidet. Der DSA macht nunmehr gar keine Aussage zur Verantwortlichkeit in ErwGr 10 DSA hinsichtlich der DSGVO. Allerding wird in den Art. 4 - 6 DAS nun der Wortlaut „haften“ statt „verantwortlich sein“ verwendet.

2. Haftungsprivilegierungen als Ausnahme zur Verantwortlichkeit?

Zumindest angedacht wurde die Anwendung der Haftungsprivilegierungen aus Art. 12 ff. e-Commerce-RL als Ausnahme zur datenschutzrechtlichen Verantwortlichkeit im Rahmen der Rechtssache Google Spain.[23] So hatte die griechische Regierung als Verfahrensbeteiligte einen Ausschluss der Verantwortlichkeit einer Suchmaschine bei ihrer Tätigkeit trotz Anerkennung einer Verarbeitung vorgeschlagen.[24] Reine Mittler von Daten könnten nicht als Verantwortliche angesehen

[23] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857.

[24] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 24. Der EuGH hatte eine Ausnahme von der Verantwortlichkeit, wie sie nach dem spanischen Recht im Zusammenhang mit der e-Commerce-RL (in Anlehnung an Art. 14 e-Commerce-RL: *van Hoboken*, Int'l J. Comm. L. &

werden, sofern eine Speicherung nur so lange wie technisch notwendig erfolge. Unklar blieb in der Darstellung der Erklärung der griechischen Regierung durch den EuGH, worauf sich dieser Ausschluss der Verantwortlichkeit gründen sollte. Aus der Definition des Verantwortlichen in Art. 2 lit. d DSRL ergab er sich jedenfalls nicht.

Denkbar wäre gewesen hinsichtlich der Suchmaschine Art. 12 Abs. 1 e-Commerce-RL zur Anwendung zu bringen.[25] Demnach wäre eine Verantwortlichkeit des Diensteanbieters[26] für die übermittelten Informationen dann nicht gegeben, wenn er kumulativ:

- a) die Übermittlung nicht veranlasst,
- b) den Adressaten der übermittelten Informationen nicht auswählt und
- c) die übermittelten Informationen nicht auswählt oder verändert.

Problematisch ist hier bereits, dass die e-Commerce-RL gem. Art. 21 Abs. 2 Suchmaschinen nicht erfassen sollte.[27] Unabhängig davon ist aber auch fraglich, ob sich das „nicht [...] verantwortlich" in Art. 12 Abs. 1 e-Commerce-RL auf die Verantwortlichkeit gemäß DSRL beziehen sollte.[28] So verwendete die DSRL[29], wie auch die DSGVO[30], in der deutschen Sprachfassung den Begriff „(für die Verarbeitung) Verantwortlicher". In der englischen Sprachfassung war die Rede vom „controller", in der französischen wiederum vom „responsable (du traitement)". Dem stand die Verwendung von „(nicht) verantwortlich" in der deutschen Sprachfassung der e-Commerce-RL gegenüber, andererseits „(not) liable" in der englischen und wieder „(ne soit pas) responsable" in der französischen. Zumindest die englische Sprachfassung der e-Commerce-RL deutete darauf hin, dass nicht die Verantwortlichkeit (responsibility) im Sinne der DSRL ausgeschlossen werden sollte, sondern die Haftung (liability). Die Aussagekraft dieses Vergleichs ist allerdings begrenzt, da gem. Art. 55 Abs. 1 EUV keine

Pol'y 2009, 2, 10) wohl konzeptionell denkbar war, nicht geprüft: *Keller*, BTLJ[33] (2018), 287, 313.

[25] Ebenso plausibel ist a., dass die Überlegung Art. 5 Abs. 1 lit. a InfoSoc-RL entstammte. Allerdings betrifft a. dieser die Übertragung in einem Netz zwischen Dritten durch einen Vermittler. Für den hier angesprochenen Fall enthielt die e-Commerce-RL aber präzisere Vorgaben.

[26] Eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln.

[27] Grabitz/Hilf[18]/*Marly*, A4 Art. 12 Vorbem. e-Commerce-RL, Rn. 9; zum Stand der Überprüfung der e-Commerce-RL 2009: *van Hoboken*, Int'l J. Comm. L. & Pol'y 2009, 2, 12 f. Der DSA enthält keine entsprechende Vorschrift, streicht Art. 21 Abs. 2 e-Commerce-RL in Art. 89 Abs. 1 DSA aber auch nicht.

[28] Vgl. *Keller*, BTLJ[33] (2018), 287, 355 f.

[29] In Art. 2 lit. d DSRL.

[30] In Art. 4 Nr. 7 DSGVO.

der Sprachfassungen von europäischen Gesetzgebungsakten Vorrang hat.[31] Dass beide Begriffe der Verantwortlichkeit voneinander unabhängig sein sollten, deckt sich auch mit dem Verständnis der Art. 29-Datenschutzgruppe.[32] Der Begriff des Verantwortlichen sei eigenständig und somit unabhängig von externen rechtlichen Quellen und anderen Rechtsgebieten, wie etwa dem Immaterialgüterrecht zu verstehen. Für den DSA scheint die Frage des Bedeutungsgehalts von „verantwortlich sein" nunmehr insoweit aufgelöst, als dass die deutsche Sprachfassung stattdessen „haften" verwendet.

3. Fazit

Die Rechtssache Google Spain bot dem EuGH die Gelegenheit darüber zu entscheiden, inwiefern die Haftungsprivilegierungen aus Art. 12 ff. e-Commerce-RL auf die DSRL übertragbar waren. Dabei ging der EuGH offensichtlich davon aus, dass die Haftungsprivilegierungen aus der e-Commerce-RL weder die Verantwortlichkeit noch die Wahrnehmung der Betroffenenrechte einschränken. Stattdessen entwickelte der EuGH im Rahmen des „Rechts auf Vergessenwerden"[33] ein Konzept, das der Haftungsprivilegierung nach Art. 14 Abs. 1 e-Commerce-RL ähnlich war, ohne dieses allerdings explizit zu erwähnen. Dieses „Recht auf Vergessenwerden" findet sich in Art. 17 DSGVO in abgeänderter Form wieder. Unklar erschien für das Verhältnis DSRL und e-Commerce-RL somit nur, ob ein Schadensersatz gem. Art. 23 DSRL aufgrund der Haftungsprivilegierungen der e-Commerce-RL eingeschränkt sein konnte.

Insgesamt schien es Konsens in der Literatur zu sein, dass die e-Commerce-RL überhaupt nicht im Anwendungsbereich der DSRL gelten sollte, insbesondere bezogen auf das Verhältnis der datenschutzrechtlichen Verantwortlichkeit zu Art. 12 ff.

[31] Zur Problematik der verschiedenen Sprachfassungen: Ehmann/Helfrich DSRL, Art. 2, Rn. 3 ff., 42 f.; m.w.N. *Cornelius*, NZWiSt 2016, 421, 424.

[32] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12.

[33] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 38 ,96.

e-Commerce-RL.[34] *Sartor* bezeichnet dies als „Datenschutz-Exzeptionalismus".[35] Konkrete Fälle, die eine Untersuchung des Verhältnisses der beiden Richtlinien notwendig gemacht hätten, bestanden bis zur Rechtssache Google Spain kaum, da Datenschutzrecht nicht in größerem Umfang zur Entfernung von Online-Inhalten genutzt wurde.[36] Teilweise wurde die Frage des Verhältnisses von DSRL und e-Commerce-RL auch dadurch umgegangen, dass man eine Verantwortlichkeit oder Auftragsverarbeitung eines Akteurs von vorneherein ablehnte, um so unproblematisch zur Anwendung der e-Commerce-RL kommen zu können.[37]

Unabhängig von der Frage der reinen Möglichkeit der Anwendung ergaben sich auch bei der tatsächlichen Anwendung der Haftungsprivilegierungen der e-Commerce-RL unmittelbar Folgeprobleme. So waren die Voraussetzungen der Privilegierungen, wie die reine Durchleitung in Art. 12 e-Commerce-RL und das Caching in Art. 13 e-Commerce-RL, umstritten.[38] Zudem wurden im Rahmen der Privilegierungen von Art. 12 ff. e-Commerce-RL nur Übermittlungen und Speicherungen erfasst, nicht aber andere Arten der Verarbeitung.[39]

II. Rechtslage zur DSGVO

Für die DSGVO wurde das Verhältnis zur e-Commerce-RL, wie oben bereits erwähnt, dadurch verkompliziert, dass Art. 2 Abs. 4 DSGVO anordnet, dass die Anwendung der e-Commerce-RL und speziell die Vorschriften Art. 12 - 15 e-Commerce-RL zur Verantwortlichkeit[40] der Vermittler durch die DSGVO unberührt bleiben.[41] Die

[34] So: *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 14; *Spindler*, JZ[69] (2014), 981, 983; *Lewinski/Herrmann*, PinG 2017, 165, 170; *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 149; *Sloot*, JIPITEC[6] (2015), 211, Rn. 2; *Keller*, BTLJ[33] (2018), 287, 304, 357 und ebd., 313: „It established what was effectively a notice-and-takedown process, without reference to Google's status as a protected intermediary under Spain's implementation of the e-Commerce Directive." Dagegen wollten andere Autoren Art. 1 Abs. 5 lit. b e-Commerce-RL so verstehen, dass die DSRL nur die Pflichten abschließend festlegte, nicht die Haftung: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1246 m.w.N.; *Sartor*, MJ[21] (2014), 564, 574.

[35] *Sartor*, IDPL[3] (2013), 3, 5.

[36] *Keller*, BTLJ[33] (2018), 287, 305, 354.

[37] Siehe *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 935, 971-973 m.w.N. mit dem Beispiel Cloud-Anbieter. Der Versuch den „unwissenden" (bzgl. des Personenbezugs) Cloud-Anbieter als Host-Provider zu privilegieren dürfte indes schon daran scheitern, dass a. die Auftragsverarbeitung kein Wissenselement voraussetzt.

[38] *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1253.

[39] *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1253.

[40] Zum Begriff: *Wielsch*, RW 2019, 84, 89 f.

[41] Zur Unverständlichkeit dieser Regelungstechnik: *Keller*, BTLJ[33] (2018), 287, 358.

üblichen Auslegungsmethoden, um den Vorrang eines Rechtsaktes zu bestimmen,[42] wie etwa die Normenhierarchie oder die Rechtsnatur der Kompetenzgrundlage, boten bei diesen beiden Sekundärrechtsakten keine Hilfestellung.[43] Um die gegenseitige „lässt die Anwendung unberührt"-Regelung aufzulösen, boten sich drei Auslegungsvarianten an.

Die erste Auslegungsvariante war, dass die Regelung in Art. 2 Abs. 4 DSGVO die Rückausnahme von Art. 1 Abs. 5 lit. b e-Commerce-RL war. Somit wären dann Art. 12 - 15 e-Commerce-RL für datenschutzrechtliche Sachverhalte wieder anwendbar gewesen.[44] Gesetzgebungstechnisch stellte sich dann allerdings die Frage, warum nicht einfach Art. 1 Abs. 5 lit. b e-Commerce-RL gestrichen werden sollte. Nach dieser Auslegungsvariante wäre etwa ein Host-Provider, der keine Kenntnis vom Personenbezug der bei ihm gehosteten Daten hätte, bis zur Erlangung der Kenntnis nicht datenschutzrechtlich für diese verantwortlich. *Van Alsenoy* verweist auf drei Argumente gegen diese Auslegung:[45] Zum einen könnten die Pflichten der Verantwortlichen und Auftragsverarbeiter auch über das Prinzip der Verhältnismäßigkeit angemessen berücksichtigt werden, so dass es nicht zu einer ausufernden Haftung komme. Zum anderen könnten die Haftungsprivilegierungen gemäß des e-Commerce-RL zu einem niedrigeren Schutz der betroffenen Personen führen. Drittens seien die Konzepte des e-Commerce-RL, also reine Durchleitung, Caching und Hosting teilweise nicht eindeutig.[46] Für den DSA lässt sich diese Auslegungsvariante nicht weiter aufrechterhalten, da der DSA statt von „verantwortlich sein" nun von „haften" spricht. Somit können sich die Privilegierungen in Art. 4 - 6 DAS systematisch nicht mehr auf die Verantwortlichkeit i.S.v. Art. 4 Nr. 7 DSGVO beziehen.

Die zweite Auslegungsvariante war, dass Art. 2 Abs. 4 DSGVO klarstellen soll, dass die Begriffe „verantwortlich" i.S.d. e-Commerce-RL und „Verantwortlicher" i.S.d. DSGVO keine Wirkung auf den jeweils anderen Rechtsakt im Rahmen seines Anwendungsbereichs haben. Haftungsprivilegierungen nach der e-Commerce-RL einerseits und der Verantwortliche nach der DSGVO andererseits wären also voneinander vollkommen unabhängig. Demnach wäre der Begriff des „verantwortlich

[42] Vgl. EuGH, Urteil vom 01.10.2019 – C-673/17 (Planet 49) = EuZW 2019, 916, Rn. 48.

[43] *Lewinski/Herrmann*, PinG 2017, 165, 170.

[44] So wohl: Kühling/Buchner/*Kühling/Raab*, Art. 2 DS-GVO, Rn. 32 m.w.N.; *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1254; *Sartor*, MJ[21] (2014), 564, 573 f.; unsicher: *Keller*, BTLJ[33] (2018), 287, 351; m.w.N. zum Meinungsstand: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1247.

[45] Noch zur e-Commerce-RL: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1248.

[46] Vgl. zu den Privilegierungen der e-Commerce-RL im Rahmen der Störerhaftung *Hacker*, MMR 2018, 779, 780 ff.

sein“ in der e-Commerce-RL nicht als Verantwortlichkeit im datenschutzrechtlichen Sinne, sondern als Haftung zu verstehen gewesen. Allgemein kann der Begriff der Verantwortlichkeit auch verschuldensunabhängige Zurechnungsgründe erfassen und sich etwa als Verschulden, Haftung, Kostenlast oder anders manifestieren.[47] In dieser Auslegungsvariante hätte die e-Commerce-RL zwar nicht für die Verantwortlichkeit allgemein, aber für die Haftung auf Schadensersatz nach Art. 82 DSGVO gegolten. Nach diesem Verständnis hätte ein Host-Provider also solange nicht für Datenschutzverstöße gem. Art. 82 DSGVO gehaftet, wie er keine Kenntnis von diesen Datenschutzverstoß hat. Dieses Verständnis lässt sich auch für den DSA weiter aufrechterhalten, da der DSA nunmehr von „haften“ statt „verantwortlich sein“ spricht.

Die dritte Auslegungsvariante war, dass Art. 2 Abs. 4 DSGVO eine rein klarstellende Wirkung haben sollte. Die DSGVO überlagere nicht die e-Commerce-RL und umgekehrt, so dass beide Rechtsakte unabhängig voneinander zu prüfen seien.[48] Die Rechtslage bleibe im Verhältnis zur DSRL insgesamt unverändert. Diese Auslegung vertrat vor allem die Kommentarliteratur aus dem Kreis der Kommission.[49] Sie deckt sich mit dem Verständnis der Art. 29-Datenschutzgruppe zur Eigenständigkeit des Begriffs des Verantwortlichen. Demnach weisen (gegenüber dem Datenschutzrecht) externe, rechtliche Quellen keine notwendige Schnittmenge mit dem Begriff des Verantwortlichen auf.[50] Somit war also denkbar, dass die e-Commerce-RL überhaupt nicht die Pflichten aus der DSGVO erfasste.[51] Dies hätte dann auch für die Haftung auf Schadensersatz nach Art. 82 DSGVO gegolten.[52] Nach diesem Verständnis wäre ein Host-Provider unabhängig von den Haftungsprivilegierungen der e-Commerce-RL verantwortlich gewesen und hätte nach Art. 82 DSGVO potenziell gehaftet. Auch dieses Verständnis lässt sich für den DSA weiter aufrechterhalten. Die dünnen Ausführungen des EuGH in der Rechtssache La Quadrature du Net[53] zu dem Verhältnis DSGVO und e-Commerce-RL sind

---

[47] *Wielsch*, RW 2019, 84, 90.

[48] So: BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, Rn. 34; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 312 ff.

[49] Ehmann/Selmayr/*Zerdick*, Art. 2 DS-GVO, Rn 19 f.; ähnlich: *Wagner*, ZD 2018, 307, 310. Die Kommission selbst hat dazu nicht Stellung bezogen: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1247.

[50] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12. Erwähnung finden etwa der Urheber oder Rechteinhaber.

[51] *Keller*, BTLJ[33] (2018), 287, 358.

[52] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 45.

[53] EuGH, Urteil vom 06.10.2020 – C-511/18 (La Quadrature du Net u.a.) = ZD 2021, 520, Rn. 212.

hingegen nur begrenzt aussagefähig, da es dort um die Frage ging, ob die Haftungsprivilegierungen der e-Commerce-RL einer Vorratsdatenspeicherung entgegenstünden.

Die ErwGr 74, 79 und 80 DSGVO enthalten in der deutschen und englischen Sprachfassung jeweils die separaten Begriffe „Verantwortung und Haftung" bzw. „responsibility and liability". Zumindest diese Sprachfassungen kennen also eine Distinktion dieser Begriffe.[54] Ebenso unterschied die Art. 29-Datenschutzgruppe bereits im WP 169[55] zwischen Verantwortlichkeit und Haftung.[56] Ungeachtet der Gleichberechtigung der Sprachfassungen gem. Art. 55 Abs. 1 EUV wird die Differenzierung zwischen Verantwortlichkeit und Haftung zudem dadurch gestützt, dass die englische Sprachfassung in Art. 2 Abs. 4 DSGVO von „liability rules" spricht, während die deutsche Fassung von „Verantwortlichkeit" und die französische von „responsabilité" spricht. Auch Art. 46 Abs. 2 lit. f und ErwGr 146 DSGVO sowie vor allem Art. 82 DSGVO scheinen darauf hinzudeuten, dass Haftung in der DSGVO weniger als Verantwortlichkeit, sondern vielmehr im Kontext von Schäden zu verstehen ist. Die e-Commerce-RL hingegen sollte grundsätzlich die Verantwortlichkeit im gesamten zivil- und strafrechtlichen Bereich regeln.[57] Im öffentlich-rechtlichen Bereich war zumindest eine Störerhaftung aufgrund der Haftungsprivilegierungen nicht ausgeschlossen.[58] Mangels Verschuldenserfordernis lässt sich die datenschutzrechtliche Verantwortlichkeit als eine solche Art der Störerhaftung verstehen. Andererseits lassen sich Betroffenenrechte im nicht-öffentlichen Anwendungsbereich der DSGVO wiederum als potenziell zivilrechtlich klassifizieren.[59] Ein weiteres systematisches Argument für die unterschiedlichen Begriffsverständnisse findet sich in Art. 21 Abs. 2 e-Commerce-RL. Dort spricht die deutsche Fassung von der „Haftung",[60] die englische von „liability" und die französische von „responsabilité". Insgesamt deutet vieles darauf hin, dass die Verantwortlichkeit in der DSGVO anders zu verstehen war als diejenige in der e-

[54] In der französischen Sprachfassung ist dies weniger deutlich, da „responsabilité" theoretisch beide Bedeutungen haben kann.

[55] Also im Geltungszeitraum der DSRL.

[56] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, 04.04.2008, 15.

[57] Grabitz/Hilf[18]/*Marly*, A4 Art. 12 Vorbem. e-Commerce-RL, Rn. 4.

[58] Spindler/Schmitz/*Spindler*, § 8 TMG, Rn. 129.

[59] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 108 ff.: „Datenschutzrecht als Verbraucherschutzrecht". Andererseits zur Einordnung des Rechts auf Vergessen werden unter Verantwortlichkeit: *Keller*, BTLJ[33] (2018), 287, 355. Allgemein: *Reimer*, DÖV 2018, 881, 881: „Bemerkenswerte Melange von Öffentlichem und Privatrecht".

[60] In seltsamer Abkehr von Art. 12 e-Commerce-RL.

Commerce-RL.[61] Unglücklich erschien die Wortwahl aufgrund der expliziten Bezugnahme von Art. 12 - 15 e-Commerce-RL in Art. 2 Abs. 4 DSGVO dennoch. Die Verwendung von „haften" statt „verantwortlich sein" in dem DSA entschärft das Verhältnis zur DSGVO nun allerdings erheblich.

Wendete man die Privilegierungen der e-Commerce-RL trotz der Auslegungsschwierigkeiten dennoch in Teilen auf die DSGVO an, stellte sich die Frage in welchem Umfang dies geschehen sollte. So war denkbar, die Privilegierungen nur auf die Haftung im Rahmen der DSGVO zu beziehen, also auf Art. 82 DSGVO.[62] Neben einer kompletten Freistellung von der Verantwortlichkeit in Art. 12 e-Commerce-RL sowie einer anteiligen Freistellung (ab Kenntnis) in Art. 13 und 14 e-Commerce-RL, wäre aber auch die Anwendung der prozeduralen Vorgaben der e-Commerce-RL ein denkbarer Anwendungsfall gewesen.[63] Demnach wären etwa Lösch- und Wiederherstellungspflichten maßgeblich gewesen und welche Kenntnis hierfür erforderlich war.

Trotz des mittlerweile deutlich weniger problematischen Wortlauts von Art. 4 - 6 DSA im Hinblick auf „haften" statt „verantwortlich sein" ist immer noch unklar, ob durch die Haftungsprivilegierungen des DSA eine Schadensersatzhaftung nach Art. 82 DSGVO ausgeschlossen werden kann. Zumindest hierfür wäre noch eine Klarstellung des Unionsgesetzgebers oder des EuGH wünschenswert.[64] Die besseren Argumente sprechen dafür, dass der Unionsgesetzgeber die Haftungsprivilegierungen des DSA nicht auf die DSGVO erstrecken wollte. Denn ohne einen Schadensersatzanspruch nach DSGVO wäre eine betroffene Person darauf angewiesen, dass eine Aufsichtsbehörde Sanktionen gegen den Verantwortlichen verhängt, sollte dieser nicht auf ihre Betroffenenrechte reagieren. Die parallele Durchsetzung des Datenschutzes durch die betroffene Person selbst sowie die Aufsichtsbehörde wäre also ohne einen nachvollziehbaren Grund eingeschränkt. Insgesamt lässt sich im Hinblick auf den neuen Wortlaut im DSA nun aber nicht mehr festhalten:

---

[61] *Lewinski/Herrmann*, PinG 2017, 165, 168, die scheinbar (zunächst, vgl. S. 170) Art. 1 Abs. 5 lit. b e-Commerce-RL übersehen, aber sich trotzdem a. für eine Parallelgeltung aussprechen.

[62] So: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 618. Vgl. a. Kühling/Buchner/*Bergt*, Art. 82 DS-GVO, Rn. 40; Simitis/Hornung/Spiecker/*Boehm*, Art. 82 DSGVO, Rn. 20; BeckOK DatenschutzR[47]/*Quaas*, Art. 82 DSGVO, Rn. 42.

[63] *Keller*, BTLJ[33] (2018), 287, 351 ff.; *Hacker*, MMR 2018, 779, 780 ff. schlägt eine teleologische Reduktion von Art. 26 Abs. 3 DSGVO anhand der Störerhaftung, auch unter Einfluss der e-Commerce-RL (mittlerweile im DSA enthalten), vor.

[64] Zur Situation unter der e-Commerce-RL noch: *Piltz*, K&R 2014, 80, 83 Fn. 28.

„Welcome to the world of Internet liability, welcome to the jungle."[65]

C. Die Verhängung von Geldbußen

Die Bedingungen für die Verhängung von Geldbußen werden in Art. 83 DSGVO geregelt. Art. 83 Abs. 2 DSGVO gibt hierbei vor, welche Umstände bei der Verhängung und der Höhe von Geldbußen Berücksichtigung finden. Art. 83 Abs. 4-6 DSGVO legen, je nach Art des Verstoßes, die Bemessungsgrenzen für die Geldbuße fest. Normadressaten von Art. 83 DSGVO sind vor allem,[66] aber nicht nur,[67] der Verantwortliche und der Auftragsverarbeiter.[68] Im Gegensatz zum Schadensersatz sehen die Vorgaben zu den Geldbußen zudem keine Gesamtschuld bei mehreren an einer Verarbeitung Beteiligten vor.[69] Insofern müssen also bei gemeinsam Verantwortlichen individuelle Geldbußen verhängt werden.

I. Der funktionale Unternehmensbegriff als Maßstab

Bei der Bemessung der Geldbuße gem. Art. 83 Abs. 4, 5 und 6 DSGVO variiert die Höchstgrenze je nachdem, ob es sich bei der bebußten Stelle um ein Unternehmen handelt oder nicht. Der Begriff Unternehmen soll dabei gem. ErwGr 150 S. 3 DSGVO im Sinne der Art. 101 und 102 AEUV als funktionaler Unternehmensbegriff verstanden werden.[70] Der funktionale Unternehmensbegriff wiederum erfasst jede eine Wirtschaftstätigkeit ausübende Einheit. Für diese Einordnung bleibt neben der Rechtsform oder der Finanzierung der Einheit auch unbeachtlich, wer genau innerhalb dieser Einheit den Verstoß zu verantworten hat.[71] Mit dem funktionalen Unternehmensbegriff werden auch Konzerne erfasst, die aus verschiedenen juristischen Personen oder Tochtergesellschaften bestehen. Damit enthält Art. 101 und 102 AEUV

[65] Noch zur Rechtslage unter der DSRL: *Sloot*, JIPITEC[6] (2015), 211, Rn. 49.

[66] *Nolde*, PinG 2017, 114, 117; *Grages*, CR 2020, 232, Rn. 5.

[67] So etwa in Art. 83 Abs. 4 lit. b und c DSGVO die Zertifizierungsstelle sowie die Überwachungsstelle.

[68] Simitis/Hornung/Spiecker/*Boehm*, Art. 83 DSGVO, Rn. 37.

[69] *Grages*, CR 2020, 232, Rn. 7, 34. Zur Frage der Beihilfe: G/S/S/V/*Feldmann*, Art. 83 DSGVO, Rn. 8.

[70] Ausführlich: Ehmann/Selmayr/*Nemitz*, Art. 83 DS-GVO, Rn. 68 ff.; *Ambrock*, ZD 2020, 492, 493 m.w.N. Kritisch: BeckOK DatenschutzR[47]/*Holländer*, Art. 83 DSGVO, Rn. 8 ff.; Auernhammer/*Golla*, Art, 83 DSGVO, Rn. 9, 36 f.; *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 174 ff.

[71] Vgl. zur Zurechnung des Handelns nach OWiG: *Hessel/Potel*, K&R 2020, 654, 655.

ein sehr weites Verständnis des Unternehmens.[72] Der Verantwortliche würde also im Hinblick auf die Geldbuße nicht nur auf eine bestimmte Art weiter qualifiziert. Vielmehr weicht der funktionale Unternehmensbegriff aus Art. 101 und 102 AEUV erheblich vom Begriff der juristischen Person innerhalb der Definition des Verantwortlichen ab.[73] Daneben weicht er auch erheblich von der Definition des Unternehmens in Art. 4 Nr. 18 DSGVO ab, denn er erfasst „jede eine Wirtschaftstätigkeit ausübende Einheit".[74] Art. 4 Nr. 18 DSGVO definiert ein Unternehmen als eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen. Während dem Unternehmensbegriff in Art. 4 Nr. 18 DSGVO eine rechtliche und formale Unternehmenskonzeption zugrunde liegt,[75] handelt es sich beim kartellrechtlichen Unternehmensbegriff um einen wirtschaftlich und funktional geprägten Begriff.[76] Das Verständnis des funktionalen Unternehmensbegriffs ähnelt also eher der Definition der Unternehmensgruppe in Art. 4 Nr. 19 DSGVO.[77] Nach dieser Definition ist eine Unternehmensgruppe eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Unklar ist, warum bei der aus ErwGr 150 S. 3 DSGVO erkennbaren Absicht nicht gleich der passendere Begriff der Unternehmensgruppe in Art. 83 DSGVO Verwendung fand.[78] Weiter verkompliziert wird die Auslegung des Unternehmensbegriffs in Art. 83 DSGVO dadurch, dass die englische Version unterschiedliche Begriffe in der Definitionsnorm Art. 4 DSGVO und in Art. 83 DSGVO verwendet. In Art. 83 DSGVO findet der Begriff „undertaking" Verwendung, in Art. 4 Nr. 18 DSGVO hingegen der Begriff „enterprise".[79] Das LG Bonn war daher aufgrund eines Vergleichs der Sprachfassungen der DSGVO der

[72] Kühling/Buchner/*Bergt*, Art. 83 DS-GVO, Rn. 20 f., 28, 39 ff.; *Artikel-29-Datenschutzgruppe*, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, 03.10.2017, 6; *Hessel/Potel*, K&R 2020, 654, 657.

[73] Trotzdem bestehe ein gewisser Gleichlauf zwischen dem Normadressat der entsprechenden Verbotsnormen und dem Subjekt der Bußgeldzumessung, so: *Cornelius*, NZWiSt 2016, 421, 424 f.

[74] Simitis/Hornung/Spiecker/*Boehm*, Art. 83 DSGVO, Rn. 40. Kritisch: G/S/S/V/*Feldmann*, Art. 83 DSGVO, Rn. 30 f.

[75] Ausführlich: *Faust/Spittka/Wybitul*, ZD 2016, 120, 120 f.

[76] *Cornelius*, NZWiSt 2016, 421, 423.

[77] Dies wird a. durch ErwGr 37 DSGVO untermauert.

[78] *Cornelius*, NZWiSt 2016, 421, 423 f. vermutet hier, aufgrund der abweichenden englischen Sprachfassung, Fehler im Gesetzgebungsverfahren.

[79] Simitis/Hornung/Spiecker/*Boehm*, Art. 83 DSGVO, Rn. 41.

Auffassung, dass der Begriff Unternehmen in Art. 83 DSGVO nicht i.S.v. Art. 4 Nr. 18 DSGVO zu verstehen ist.[80]

Legt man das dargestellte Verständnis zugrunde, könnte also bspw. die irische Tochtergesellschaft einer amerikanischen Muttergesellschaft Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO sein, während für die Bemessung der Geldbuße nach Art. 83 DSGVO nicht nur die eigentlich verantwortliche Tochtergesellschaft, sondern auch die Muttergesellschaft und der restliche Konzern herangezogen wird. Demnach würden also Verantwortlicher und Sanktionierter zwar nicht komplett auseinanderfallen, sie wären aber jedenfalls personell nicht mehr kongruent. Allein aus einem kartellrechtlich beherrschenden Einfluss der Muttergesellschaft kann aber nicht zwangsläufig auch auf die datenschutzrechtliche Entscheidung der Muttergesellschaft über Zwecke und Mittel der Verarbeitung geschlossen werden.[81] Eine Verantwortlichkeit der Muttergesellschaft kommt dann in Frage, wenn sie selbst die Entscheidung über Zwecke und Mittel der Verarbeitung trifft, allerdings wäre dann wiederum nicht die Tochtergesellschaft notwendigerweise gemeinsam verantwortlich. Treffen Muttergesellschaft und Tochtergesellschaft tatsächlich gemeinsam die Entscheidung über Zwecke und Mittel der Verarbeitung, dann können diese unproblematisch gemeinsam Verantwortliche sein. Aber selbst in diesem Szenario würde man nicht unbedingt zu einer Kongruenz zwischen Geldbußenbemessung und Verantwortlichkeit kommen, da dann immer noch fraglich wäre, ob auch die anderen Teile des Konzerns neben der entsprechenden Mutter- und Tochtergesellschaft einen Entscheidungsbeitrag für eine gemeinsame Verantwortlichkeit erbracht hätten. Ungeachtet dessen wäre auch noch die Frage des anwendbaren Rechts und die Zuständigkeit der Aufsichtsbehörde, die sich nur anhand der Niederlassung ergeben kann, zu prüfen. Im Ergebnis würde also der Verantwortliche als Sanktionierter und die Bemessungsgröße des Unternehmens für die Sanktion potenziell auseinanderfallen.[82]

Gegen die Verwendung des funktionalen Unternehmensbegriffs in Art. 83 DSGVO spricht, dass es in der DSGVO kein dem Kartellrecht entsprechendes Konzernprivileg gibt.[83] Zudem stellt sich ein systematisches Problem insoweit, dass sich ein Erwägungsgrund über eine Legaldefinition hinwegsetzt.[84] Dies gilt jedenfalls dann, wenn man annimmt, dass der Begriff Unternehmen in Art. 83 DSGVO tatsächlich auf

[80] LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20 = MMR 2021, 173, Rn. 59.
[81] *Hessel/Potel*, K&R 2020, 654, 655 f.
[82] Unproblematisch scheinbar: *Grages*, CR 2020, 232, Rn. 6.
[83] *Cornelius*, NZWiSt 2016, 421, 425.
[84] Vertiefend: *Cornelius*, NZWiSt 2016, 421, 423.

die Definition in Art. 4 Nr. 18 DSGVO verweist. Andererseits würde als Folge der Anwendung des funktionalen Unternehmensbegriffs der globale Konzernumsatz berücksichtigt werden, was wiederum Anklang im Tatbestandsmerkmal „weltweit" in Art. 83 Abs. 4-6 DSGVO findet. Insgesamt bestehen aber jedenfalls Zweifel an der Bestimmtheit der Norm, die gem. Art. 49 GRCh auch im Unionsrecht Voraussetzung für eine solche Sanktion ist.[85]

Aufgrund der erheblichen Unterschiede zwischen den maßgeblichen kartellrechtlichen und datenschutzrechtlichen Normen wird eine Kompromisslösung dergestalt vorgeschlagen, dass eine datenschutzrechtliche Einheit für die Verhängung der Geldbuße vorausgesetzt werden soll. Ein einflussreicheres Unternehmen soll also ein anderes Unternehmen zur Einhaltung datenschutzrechtlicher Vorgaben verpflichten können müssen.[86] Dies würde im Hinblick auf das Urteil des EuGH in der Rechtssache Jehovan todistajat[87] allerdings wiederum auf eine gemeinsame Verantwortlichkeit hindeuten. Bei einer gemeinsamen Verantwortlichkeit müssten dann konsequenterweise Geldbußen an die individuell Verantwortlichen, also etwa die Konzernmutter sowie die Konzerntochter, vergeben werden, anstelle einer einheitlichen Bemessungsgröße.[88] Daneben wird erwogen, den funktionalen Unternehmensbegriff teleologisch auf den Umfang der Verantwortlichkeit gem. Art. 4 Nr. 7 DSGVO zu reduzieren.[89] Dies wird zum einen mit dem Grundsatz der Verhältnismäßigkeit begründet, andererseits aber auch damit, dass sich der Schadensersatz aus Art. 82 DSGVO nicht am funktionalen Unternehmensbegriff orientiere. Das letzte Argument übersieht dabei, dass es sich hier um zwei völlig unterschiedliche Mechanismen handelt. Der Schadensersatz hat im Gegensatz zur Geldbuße keinen sanktionierenden, sondern einen Genugtuungs- und Reparationscharakter. Daneben macht die teleologische Reduktion aber auch ErwGr 150 S. 3 DSGVO überflüssig. Eine klare Linie in der Rechtsprechung ist bislang noch nicht auszumachen. Das LG Bonn hatte sich in einer Entscheidung nicht weiter mit den spezifisch datenschutzrechtlichen Voraussetzungen des Verweises auf den funktionalen Unternehmensbegriff in ErwGr 150 S. 3 DSGVO auseinandergesetzt.[90]

---

[85] LG Berlin, Beschluss vom 18.02.2021 – 212 Js-OWi 1/20 = BeckRS 2021, 2985, Rn. 24; *Krohm*, RdV 2017, 221, 223 f.

[86] *Cornelius*, NZWiSt 2016, 421, 425 f.; *Nolde*, PinG 2017, 114, 116; *Krohm*, RdV 2017, 221, 225.

[87] Dazu: Kapitel 4 B. II. Jehovan todistajat.

[88] So wohl a. *Krohm*, RdV 2017, 221, 225 f., der unterstreicht, dass keine Geldbuße anhand des Gesamtumsatzes zu bemessen sei, sondern die Bemessung individuell für die gemeinsam Verantwortlichen zu erfolgen habe.

[89] *Hessel/Potel*, K&R 2020, 654, 657 f.

[90] LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20 = MMR 2021, 173, Rn. 58.

Unabhängig von der Frage, ob der Verweis auf den Unternehmensbegriff aus Art. 101 und 102 AEUV dem Bestimmtheitsgebot genügt, erscheint eine getrennte Bestimmung von Verantwortlichkeit und Bußgeldbemessung notwendig.[91] Dies hat nunmehr auch der EuGH durch Urteil in der Rechtssache Deutsche Wohnen bestätigt.[92] Der Unternehmensbegriff aus Art. 101 und 102 AEUV sei nur relevant, um die Höhe einer Geldbuße gem. Art. 83 Abs. 4-6 DSGVO zu bestimmen. Dies heißt im Umkehrschluss allerdings auch, dass der funktionale Unternehmensbegriff nicht zur Bestimmung des Verantwortlichen nach Art. 4 Nr. 7 DSGVO genutzt werden kann.[93] Abgesehen von der Möglichkeit einer gemeinsamen Verantwortlichkeit lässt sich also auch keine Verantwortlichkeit eines Konzerns begründen.[94] Deutlich wird demnach bei der Bemessung der Geldbuße, dass der Verantwortliche hier trotz seiner Funktion als primärer Adressat der DSGVO keine gravierende Rolle übernimmt.

II. Weitere Voraussetzungen des OWiG vs. DSGVO

Nach deutschem Recht bestehen zudem Widersprüche zwischen § 30 Abs. 1 OWiG[95] und Art. 83 DSGVO für die Verhängung von Geldbußen. Gegenstand der Geldbuße nach Art. 83 DSGVO ist der Verstoß als Erfolg (Erfolgsunrecht), so dass die DSGVO nicht eine spezifische Handlung des Verantwortlichen oder seiner einzelnen Teile sanktioniert (Handlungsunrecht).[96] Dieser Verstoß wird dem Verantwortlichen als Organisationseinheit zugerechnet. Das deutsche OWiG als Sanktionsrecht kennt eine solche unmittelbare Haftung von juristischen Personen allerdings bislang nicht.[97] Zwar kann gem. § 30 Abs. 1 OWiG eine Geldbuße auch gegen juristische Personen oder Personenvereinigung verhängt werden, allerdings knüpft diese Geldbuße dann an ein schuldhaftes Fehlverhalten im Sinne einer Handlung einer natürlichen Person an.[98] Im Gegensatz zur organisatorischen Zuordnung eines Verstoßes entsprechend zum Konzept des Verantwortlichen, muss also für § 30 Abs. 1 OWiG eine individualisierbare Handlung einer natürlichen Person vorliegen.[99] Zusätzlich muss

[91] Kühling/Buchner/*Bergt*, Art. 83 DS-GVO, Rn. 28. Ähnlich wie das Vorgehen bei: *Hessel/Potel*, K&R 2020, 654, 656 f.

[92] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 54 ff.

[93] Insofern richtig: *Hessel/Potel*, K&R 2020, 654, 657.

[94] Vgl. EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 30.

[95] Daneben a. § 30 Abs. 4 und § 130 OWiG.

[96] Vgl. *Bull*, NJW[32] (1979), 1177, 1180 zum Verständnis des Datenschutzrechts als Gefährdungsrecht.

[97] Auernhammer/*Golla*, Art, 83 DSGVO, Rn. 8 sieht hier die Notwendigkeit einer unionsrechtskonformen extensiven Auslegung.

[98] Die juristische Person oder Personenvereinigung haftet dann als Nebenbetroffene.

[99] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung

dieses Fehlverhalten im Rahmen des § 30 Abs. 1 OWiG von bestimmten Personen in Führungs- oder Aufsichtspositionen begangen werden. Es muss sich dabei gem. § 30 Abs. 1 Nr. 5 OWiG grundsätzlich um ein Organ oder eine Person mit Leitungsaufgaben der juristischen Person oder Personenvereinigung handeln. Eine Haftung für weitere juristische Personen eines Konzerns im Sinne einer Verbandshaftung ist im OWiG nicht vorgesehen. Nach dem Funktionsträgerprinzip aus Art. 101 und 102 AEUV haftet hingegen das Unternehmen unmittelbar. Ein individualisierbarer Vorwurf im Rahmen einer Kenntnis oder Anweisung der Unternehmensleitung oder die Verletzung einer Aufsichtspflicht ist nicht erforderlich.

Ob Art. 83 DSGVO die Vorgaben des § 30 Abs. 1 OWiG aufgrund des Konzeptes des Verantwortlichen gem. Art. 4 Nr. 7 DSGVO oder des Verweises auf Art. 101 und 102 AEUV in ErwGr 150 S. 3 DSGVO überschreibt, stand bis zur Entscheidung des EuGH in der Rechtsache Deutsche Wohnen[100] nicht fest.[101] § 41 Abs. 1 BDSG ordnet die sinngemäße Geltung der Vorschriften des OWiG für die Verhängung von Geldbußen nach Art. 83 Abs. 4-6 DSGVO an. Zwar legt § 41 Abs. 1 S. 2 BDSG fest, dass bestimmte Normen des OWiG keine Anwendung finden, allerdings erfasst dies nicht § 30 Abs. 1 OWiG.

Weil Art. 83 Abs. 4-6 DSGVO die Voraussetzungen der Zurechnung eines Verstoßes vermeintlich nicht abschließend regeln solle, wurde vertreten, dass insoweit Raum für mitgliedstaatliches Recht wie § 30 Abs. 1 OWiG bestehe.[102] Die Zurechnung über § 30 Abs. 1 OWiG sei erforderlich, weil eine juristische Person nicht selbst, sondern nur durch ihre Organe und Vertreter handeln könne, gleichzeitig aber die rechtswidrige und vorwerfbare Handlung Voraussetzung für ein Bußgeld nach § 1 Abs. 1 OWiG sei.[103] ErwGr 150 S. 3 DSGVO und die damit verbundene unmittelbare Verbandshaftung sei unbeachtlich, da es dort um die Höhe der Geldbuße, nicht aber die Voraussetzungen ihrer Verhängung gehe.[104] Gleichzeitig wurde aber auch vertreten, dass Art. 83 DSGVO dem Modell einer unmittelbaren Verbandshaftung im Sinne des bereits erwähnten funktionalen Unternehmensbegriffs folge.[105] Für letztere Ansicht sprach neben dem Verweis in ErwGr 150 S. 3 DSGVO auf Art. 101 und 102 AEUV

Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20 f.

[100] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203. Dazu gleich.

[101] Einerseits: LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20 = MMR 2021, 173, Rn. 22 ff.; andererseits: LG Berlin, Beschluss vom 18.02.2021 – 212 Js-OWi 1/20 = BeckRS 2021, 2985, Rn. 10 ff.

[102] Sydow/Marsch/*Popp*, Art. 83 DSGVO, Rn. 6 m.w.N. LG Berlin, Beschluss vom 18.02.2021 – 212 Js-OWi 1/20 = BeckRS 2021, 2985, Rn. 10 f., 15.

[103] LG Berlin, Beschluss vom 18.02.2021 – 212 Js-OWi 1/20 = BeckRS 2021, 2985, Rn. 16.

[104] LG Berlin, Beschluss vom 18.02.2021 – 212 Js-OWi 1/20 = BeckRS 2021, 2985, Rn. 23.

[105] Kühling/Buchner/*Bergt*, Art. 83 DS-GVO, Rn. 20 m.w.N.

auch die explizite Erwähnung des Verantwortlichen, des Auftragsverarbeiters sowie zwei weiterer Adressaten in Art. 83 DSGVO. Diesen Adressaten ist gemein, dass sie alle keine natürliche Personen sind. Mit dem Modell einer unmittelbaren Verbandshaftung, wie sie Art. 83 DSGVO voraussetze, sei § 30 Abs.1 OWiG daher nicht vereinbar. Folglich solle diese Norm aufgrund des unionsrechtlichen Effektivitätsgebots nicht zur Anwendung kommen.[106]

Problematisch erschien dabei noch, inwiefern der Verweis auf das mitgliedstaatliche Verfahrensrecht in Art. 83 Abs. 8 DSGVO einen Rückgriff auch auf materiell-rechtliche Vorschriften im OWiG, also eben § 30 Abs. 1 OWiG, ermöglichte. Das LG Bonn war der Auffassung, dass dieser Verweis im Rahmen des unionsrechtlichen Effektivitätsgebots auszulegen sei.[107] Sofern also mitgliedstaatliches Recht im Bereich des Bußgeldverfahrens der Durchsetzung einer Geldbuße nach Art. 83 DSGVO widersprechen sollte, komme es nicht zur Anwendung. Art. 83 Abs. 8 DSGVO beziehe sich zudem explizit nur auf das Bußgeldverfahren, nicht auf materielles Recht. Das LG Berlin nahm eine solche Einschränkung hingegen nicht vor und wendete Art. 83 Abs. 8 DSGVO auch auf § 30 Abs. 1 OWiG i.V.m. § 41 Abs. 1 S. 1 BDSG an.[108] Das BMI schließlich ging davon aus, § 30 Abs. 1 OWiG zurecht nicht von dem Verweis in § 41 Abs. 1 BDSG ausgenommen zu haben.[109] ErwGr 150 S. 3 DSGVO regele nur die Bemessung der Geldbuße, nicht aber die Adressaten der Geldbuße.

Der EuGH hat mittlerweile zu dem Vorlageverfahren des KG Berlin im weiteren Instanzenzug des Beschlusses des LG Berlins entschieden.[110] Zunächst unterscheide die DSGVO hinsichtlich der Haftung Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO nicht zwischen natürlichen und juristischen Personen.[111] Voraussetzung sei allein, dass es sich bei dem Haftenden um einen Verantwortlichen im Sinne der Definition handele. Es müsse möglich sein Geldbußen gem. Art. 83 DSGVO unmittelbar gegen juristische Personen zu verhängen, sofern diese ein Verantwortlicher seien.[112] Die materiellen Voraussetzungen für das Verhängen einer Geldbuße seien in Art. 58 Abs. 2, Art. 83 Abs. 1-6 DSGVO genau und ohne Ermessenspielraum der Mitgliedstaaten

[106] LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20 = MMR 2021, 173, Rn. 23 ff.; Kühling/Buchner/*Bergt*, § 41 BDSG, Rn. 7 m.w.N.

[107] LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20 = MMR 2021, 173, Rn. 35.

[108] LG Berlin, Beschluss vom 18.02.2021 – 212 Js-OWi 1/20 = BeckRS 2021, 2985, Rn. 15.

[109] *Piltz*, https://www.delegedata.de/2021/11/bundesinnenministerium-dsgvo-bussgelder-muessen-nach-den-vorgaben-des-deutschen-owig-verhaengt-werden/ (abgerufen am 17.07.2024).

[110] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203.

[111] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 42 f.

[112] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 44.

aufgeführt.[113] Es bestehe insbesondere keine Bestimmung in der DSGVO, die die Verhängung einer Geldbuße gegen eine juristische Person als Verantwortliche davon abhängig mache, dass zuvor festgestellt werde, dass dieser Verstoß von einer identifizierten natürlichen Person begangen wurde.[114] Die durch Art. 58 Abs. 4, Art. 83 Abs. 8 DSGVO eingeräumte Möglichkeit der Mitgliedstaaten, Anforderungen an das von den Aufsichtsbehörden anzuwendende Verfahren bei der Verhängung einer Geldbuße vorzusehen, bedeute aber keineswegs, dass die Mitgliedstaaten auch befugt wären, über verfahrensrechtlichen Anforderungen hinaus materiell-rechtliche Voraussetzungen vorzusehen zusätzlich zu denen in Art. 83 Abs. 1-6 DSGVO.[115] Es bestehe ausdrücklich kein Spielraum hinsichtlich der materiellen Voraussetzungen. Dies ergebe sich auch aus dem Zweck der DSGVO.[116]

III. Fazit

Die Rechtsprechung des EuGH im Hinblick auf Geldbußen gem. Art. 83 DSGVO gegen juristische Personen ist schlüssig und dient einer effektiven Verhängung durch die Aufsichtsbehörden. Hinsichtlich seiner obiter dictum-Ausführungen zu der Bewandtnis des Unternehmensbegriffs aus Art. 101 und 102 AEUV im Kontext von Geldbußen macht es sich der EuGH allerdings etwas zu einfach. So ist nach wie vor unklar, wie dieser Unternehmensbegriff bei Geldbußen für gemeinsam Verantwortlichen, die Teil desselben Unternehmens i.S.v. Art. 101 und 102 AEUV sind, zu verstehen ist. Sinnvoll scheint es hier die Gesamtschuld eines gemeinsam Verantwortlichen innerhalb der wirtschaftlichen Einheit anzunehmen bzw. eine teleologische Reduktion insoweit vorzunehmen, dass eine wirtschaftliche Einheit trotz mehrerer Verantwortlicher nur einmal bebußt werden kann.

[113] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 45.
[114] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 46.
[115] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 47 f.
[116] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203, Rn. 49 ff.

Kapitel 4

Gemeinsam mit anderen (Verantwortlichen)

Der Verantwortliche kann gemäß der Definition in Art. 4 Nr. 7 DSGVO nicht nur allein, sondern auch gemeinsam mit anderen (Verantwortlichen) über die Zwecke und Mittel der Verarbeitung entscheiden. In diesem Abschnitt soll das Definitionselement „gemeinsam mit anderen" als solches analysiert werden.

Besteht aufgrund der Beteiligung mehrerer Akteure an einem Sachverhalt die Möglichkeit, einzelne Voraussetzungen zwischen den Akteuren wechselseitig zuzurechnen, erhöht sich naturgemäß die Komplexität[1] einer Analyse.[2] Dies gilt umso mehr, wenn unklar ist, welche Mindestvoraussetzungen ein Akteur für sich genommen erfüllen muss, damit eine solche Zurechnung überhaupt erfolgen kann. Beides zeigt sich besonders deutlich bei den gemeinsam Verantwortlichen.[3]

Obwohl, ausgehend vom Wortlaut, nur die Entscheidung über das Element „gemeinsam (mit anderen)" weiter qualifiziert wird,[4] ist die Feststellung einer gemeinsamen Verantwortlichkeit ungemein schwieriger als die einer singulären Verantwortlichkeit.[5] Art. 26 DSGVO, als spezifische Regelung der gemeinsam Verantwortlichen, verlangt zwar eine Vereinbarung zwischen den gemeinsam Verantwortlichen, allerdings ist diese nicht konstitutiv für die gemeinsame Verantwortlichkeit.[6] Sie ist vielmehr Folge einer faktischen gemeinsamen Verantwortlichkeit. Erforderlich ist auch nicht eine spezifische Entscheidung der beteiligten Akteure für eine gemeinsame Verantwortlichkeit, sondern schlicht die tatsächliche gemeinsame Entscheidung über die Zwecke und Mittel einer Verarbeitung.[7] Diese gemeinsame Entscheidung wird, wie bei der Entscheidung

[1] Vgl. *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 141 ff. zur Verantwortlichkeitszuschreibung als Form von Komplexitätsmanagement.

[2] Zu potenziellen Anwendungsfällen ausführlich: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 4 ff.

[3] *Monreal*, CR 2019, 797, Rn. 38.

[4] Sydow/Marsch/*Ingold*, Art. 26 DSGVO, Rn. 4.

[5] Unabhängig davon will der EDPB die Voraussetzungen der gemeinsam Verantwortlichen ggü. den des singulär Verantwortlichen spiegelbildlich verstehen: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 50.

[6] Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 22 m.w.N.

[7] Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 13 m.w.N.

allgemein, anhand aller Umstände ermittelt, aus denen ein Einfluss auf die Verarbeitung abgeleitet werden kann.[8]

Notwendig ist im Hinblick auf das Element der Entscheidung eine Entscheidungsmacht, die sich in dem Einfluss auf die Verarbeitung, präziser auf deren Zwecke und Mittel, zeigt. Denn das „gemeinsam mit anderen [...] entscheidet" in Art. 4 Nr. 7 DSGVO bezieht sich rein grammatikalisch auf die „Zwecke und Mittel der Verarbeitung". Wie stark diese Entscheidungsmacht bzw. der Einfluss sein muss, damit von einem gemeinsam Verantwortlichen gesprochen werden kann, ist abseits einer Parität der gemeinsam Verantwortlichen weitgehend unklar.[9] Vor allem diese Frage beherrscht daher die Diskussion um die gemeinsame Verantwortlichkeit.[10] Teilweise wird das Element „gemeinsam (mit anderen)" allerdings auch so verstanden, dass es sich auf die Zwecke und/oder Mittel der Verarbeitung bezieht. Nach diesen Ansichten müssen dann entweder gemeinsame Zwecke,[11] gemeinsame Mittel[12] oder sogar beides[13] vorliegen. Erachtet man die Entscheidungsmacht als maßgebliche Voraussetzung für einen Verantwortlichen, erscheint wenigstens ein gemeinsamer Zweck oder ein gemeinsames Mittel erforderlich. Denn ansonsten stellt sich die Frage, zu was der Entscheidungsbeitrag eines gemeinsam Verantwortlichen überhaupt erfolgen soll.[14] Soweit nur ein gemeinsamer Zweck oder nur gemeinsame Mittel vorliegen, muss allerdings der fremde Entscheidungsbeitrag zu den nicht gemeinsamen Zwecken oder Mitteln auch gebilligt werden.[15] Wie sich eine solche Billigung ableiten lässt, ergibt sich unter anderem aus dem Konzept der Zweckkomplementarität.[16] Für die Bestimmung eines gemeinsam Verantwortlichen sind daneben Indizien für eine Abgrenzung zum Auftragsverarbeiter essenziell.[17] Zudem stellt sich die Frage, wann ein Auftragsverarbeiter-[18] oder Mitarbeiterexzess vorliegt, der potenziell eine gemeinsame Verantwortlichkeit zur Folge haben kann. Die gemeinsame Verantwortlichkeit muss

[8] Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 47.

[9] Dazu: Kapitel 4 I. Erheblichkeitsschwelle des Entscheidungsbeitrags. Siehe etwa: *Kartheuser/Nabulsi*, MMR 2018, 717, 718.

[10] *Moos/Rothkegel*, MMR 2019, 584, 585.

[11] Dazu: Kapitel 4 E. Die Zwecke der Verarbeitung als Entscheidungsobjekt.

[12] Dazu: Kapitel 4 F. Die Mittel der Verarbeitung als Entscheidungsobjekt.

[13] Dazu: Kapitel 4 C. C. Vorfragen - „Gemeinsam" im Kontext der Definition.

[14] Dazu: Kapitel 4 H. III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung.

[15] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

[16] Dazu: Kapitel 4 E. I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen.

[17] Dazu: Kapitel 4 J. Indizien für eine Abgrenzung zum Auftragsverarbeiter.

[18] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

also auf der einen Seite zum Auftragsverarbeiter abgegrenzt werden. Auf der anderen Seite muss sie zu separaten Verantwortlichen, zwischen denen nur eine Übermittlung stattfindet, abgegrenzt werden.[19] Vor allem aber stellt sich die Frage, wie die gemeinsame Entscheidung insgesamt als Prozess oder Handlung zu verstehen ist.[20] Schließlich sind die Folgen einer gemeinsamen Verantwortlichkeit zu klären.[21] Zuletzt erfolgt eine Bewertung der Analyse.[22] Zunächst erfolgt aber als allgemeine Einführung[23] eine Aufnahme des Erkenntnisstandes zu den gemeinsam Verantwortlichen vor Geltungsbeginn der DSGVO[24] sowie eine Darstellung der Entscheidungen des EuGH zur gemeinsamen Verantwortlichkeit.[25]

A. Die Quellenlage vor Geltungsbeginn der DSGVO

I. Literatur

Wie bereits dargestellt, fanden die gemeinsam Verantwortlichen erstmalig in der DSRL Erwähnung.[26] In der deutschen prä-DSGVO Literatur fand sich, abseits von den drei DSRL-Kommentaren,[27] kaum ein Hinweis auf die gemeinsam Verantwortlichen.[28] In einem dieser Kommentare wurden die nicht rechtsfähigen Personengemeinschaften[29] als möglicher Anwendungsfall erwähnt.[30] Mangels einer weiteren Begründung dürfte dies bereits mit der Definition selbst im Widerspruch stehen. Denn diese zählt neben der juristischen Person explizit verschiedene Organisationseinheiten, so etwa die Stelle, auf. Daneben sind Begriffe wie die juristische Person ohnehin unionsrechtsautonom auszulegen, so dass auch eine nicht rechtsfähige Personengemeinschaft möglicherweise

[19] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 24.

[20] Dazu: Kapitel 4 H. Die gemeinsame Entscheidung.

[21] Dazu: Kapitel 4 L. Folgen der gemeinsamen Verantwortlichkeit.

[22] Dazu: Kapitel 4 M. Schlussfolgerungen aus der Analyse - Die Unterkomplexität des Verantwortlichkeitskonzeptes.

[23] Dies dient auch der Verständlichkeit der Urteile sowie der Vermeidung von Wiederholungen.

[24] Dazu: Kapitel 4 A. Die Quellenlage vor Geltungsbeginn der DSGVO.

[25] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[26] Dazu: Kapitel 1 B. V. DSRL (1995).

[27] Dammann/Simitis (Hrsg.), EG-Datenschutzrichtlinie, 1997, Ehmann/Helfrich (Hrsg.), EG-Datenschutzrichtlinie, 1999 und Grabitz/Hilf[40]/*Brühann*, A 30 Vorbem. DSRL.

[28] Vgl. BeckOK DatenschutzR[28]/*Spoerr*, § 11 BDSG a.F., Rn. 64 ff.; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 5, 13; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 23; *Kartheuser/Nabulsi*, MMR 2018, 717, 718.

[29] Also etwa Erbengemeinschaft, Bruchteilsgemeinschaft oder Innen-GbR.

[30] Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 11.

hierunter fallen könnte. Laut einem anderen Kommentar sei ein Anwendungsfall der gemeinsam Verantwortlichen vor allem die Nutzung von Datenverbundnetzen durch mehrere Partner.[31] Schließlich wurde darauf hingewiesen, dass eine gemeinsame Verantwortlichkeit etwa dann vorliegen könne, wenn die Entscheidung über die Zwecke einerseits und über die Mittel andererseits auseinanderfalle.[32] Diese Ansicht wurde zwar von der Art. 29-Datenschutzgruppe später in WP 169 aufgegriffen,[33] von ihrem Nachfolgegremium, dem EDPB,[34] für die DSGVO allerdings anscheinend nicht weiterverfolgt.[35] Gewinnbringende Erkenntnisse zur gemeinsamen Verantwortlichkeit konnten der prä-DSGVO Literatur insgesamt nicht entnommen werden.

II. Die mangelhafte Umsetzung der DSRL

Ein Grund für die fehlende Aufarbeitung des Konzeptes der gemeinsamen Verantwortlichkeit im deutschen Recht könnte darin liegen, dass der deutsche Gesetzgeber bei der Umsetzung der DSRL in das BDSG[36] versäumt hatte die gemeinsam Verantwortlichen explizit wenigstens in die Definitionen aufzunehmen.[37] So wurde bei der Umsetzung der DSRL 2001 die „speichernde Stelle" aus § 3 Abs. 8 BDSG 1990 durch die „verantwortliche Stelle" sowie „speichert" durch „erhebt, verarbeitet oder nutzt" ersetzt. Man kann also hinsichtlich der Definition des Verantwortlichen von einem minimalen Anpassungswillen sprechen.[38] Bis zum Außerkrafttreten des BDSG a.F. mit Geltungsbeginn der DSGVO 2018 erfolgte keine weitere Änderung der Definition. Neben der fehlenden Erwähnung der gemeinsam Verantwortlichen insgesamt dürfte auch deren systematische Begründung im Hinblick auf das in der deutschen Definition fehlende Element der Entscheidung schwergefallen sein. Die Frage, ob eine gemeinsame Verantwortlichkeit vorliegt, stellt sich definitionsgemäß nämlich nicht bereits dann, wenn ein Akteur irgendeinen Bezug zu

[31] Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 19.

[32] Dieser Fall wird aber als eher unwahrscheinlich erachtet.

[33] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23.

[34] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 36, 51, 53.

[35] Dazu: Kapitel 4 H. III. 4. Das Verständnis der gemeinsamen Entscheidung nach Auffassung der Aufsichtsbehörden.

[36] Dazu: Kapitel 1 B. VI. BDSG (2001).

[37] *Gierschmann*, ZD 2020, 69, 69.

[38] Siehe BT-Drs. 14/4329, S. 33; dies geschah in Verkennung des unionsrechtsautonomen Verständnisses des Begriffs: *Monreal*, CR 2019, 797, Rn. 17; vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

einer Verarbeitung hat, sondern wenn sich konkret Berührungspunkte mit den Zwecken und Mitteln der Verarbeitung ergeben. Ausgehend von diesen unterschiedlichen Definitionen des Verantwortlichen in DSRL und BDSG a.F. scheint die fachliche Diskussion über die gemeinsam Verantwortlichen in Deutschland noch heute häufig einer präzisen Orientierung an den verschiedenen Definitionselementen zu entbehren.

III. Die Weiterleitung bei mehreren speicherberechtigten Stellen nach § 6 Abs. 2 BDSG a.F. als gemeinsame Verantwortlichkeit?

In der Literatur finden sich vereinzelte Verweise darauf, dass die gemeinsam Verantwortlichen, unabhängig von § 3 Abs. 7 BDSG 2001, in § 6 Abs. 2 BDSG 2001[39] bereits erkennbar gewesen wären.[40] § 6 Abs. 2 BDSG 2001 regelte, dass sich der Betroffene an verschiedene speicherungsberechtigte Stellen wenden konnte, wenn er nicht feststellen konnte, welche Stelle die Daten gespeichert hatte. Diese Stellen waren dann verpflichtet, das Vorbringen des Betroffenen an die tatsächlich speichernde Stelle weiterzuleiten. Diese Autoren lassen allerdings außer Acht, dass die Zuständigkeitsregelung aus Art. 26 Abs. 3 DSGVO, zu der § 6 Abs. 2 BDSG 2001 gewisse Ähnlichkeiten aufwies, in der DSRL nicht vorhanden war. Es handelte sich bei § 6 Abs. 2 BDSG 2001 nur um eine Erleichterung der Durchsetzung der Betroffenenrechte, allerdings ohne die Verbindung zu gemeinsam Verantwortlichen.[41] § 6 Abs. 2 BDSG a.F. konnte somit als Kompensationsnorm für die mangelnde Feststellbarkeit bzw. Transparenz des singulären Verantwortlichen verstanden werden. Ähnliche Beispiele für eine solche Zuständigkeitsregelung bei singulären Verantwortlichen finden sich etwa noch heute in den gemeinsamen Verbunddateien deutscher Sicherheitsbehörden, bspw. der Antiterrordatei oder der gemeinsamen

[39] „Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten."

[40] G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 25; *Dovas*, ZD 2016, 512, 513. Kritisch: *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 457. *Weichert*, 9.5 Chipkarten, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 25 ff. verlangt statt gemeinsam Verantwortlicher vielmehr die genaue Protokollierung der Verarbeitung um den jeweils Verantwortlichen zu bestimmen.

[41] Vgl. Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 4. Fernliegend daher: G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 25.

Dateien des BfV und der LfVs.[42] Abseits der Verpflichtung zur Weiterleitung des Vorbringens des Betroffenen ergaben sich aus § 6 Abs. 2 BDSG 2001 keine weiteren Pflichten an.[43] Folglich waren keine aufsichtsbehördlichen Maßnahmen gegenüber der weiterleitenden Stelle möglich. Auch die Prüfungspflichten in §§ 15, 16 BDSG 2001 zur Datenübermittlung stellten keine Vorstufe der gemeinsam Verantwortlichen dar. Es handelte sich vielmehr nur um Voraussetzungen für eine Übermittlung.[44] Unabhängig von der Beteiligung mehrerer Akteure an einem Verarbeitungsszenario liegt aber noch keine gemeinsame Verantwortlichkeit vor, wenn nicht tatsächlich die Verantwortung für wenigstens einen Verarbeitungsvorgang geteilt wird.[45] Insofern ging das BDSG 2001 auch in den genannten Vorschriften immer noch von einem singulären Verantwortlichen aus.[46] Dass es sich bei diesen Normen nicht um eine Umsetzung der gemeinsamen Verantwortlichkeit handeln kann, wird insbesondere dann klar, wenn man das Alter der Normen bedenkt. Sowohl § 6 Abs. 2 BDSG 2001 als auch §§ 15, 16 BDSG 2001 waren bereits im BDSG 1990 enthalten, also vor Verabschiedung der DSRL, die die gemeinsame Verantwortlichkeit erstmals gesetzlich definierte.

B. Rechtsprechung des EuGH

Vermutlich aufgrund der dieser mangelhaften Umsetzung der DSRL gab es in Deutschland während des Geltungszeitraums der DSRL kaum Entscheidungen zur gemeinsamen Verantwortlichkeit.[47] Der EuGH hingegen hat, zwar schon nach Verabschiedung der DSGVO, aber noch zur Rechtslage unter der DSRL, drei Urteile gefällt, die sich mit den gemeinsam Verantwortlichen beschäftigten. Diese Urteile ergingen in den Rechtssachen Wirtschaftsakademie, Jehovan todistajat und Fashion ID. Zur Rechtslage unter der DSGVO folgten zwei weitere Urteile in den Rechtssachen

[42] Dazu: Kapitel 2 F. VII. Anwendungsfälle? Vgl. § 8 Abs. 1 S. 2 ATDG; § 6 Abs. 2 S. 6 BVerfSchG.
[43] Vgl. G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 27.
[44] Deutlich insofern hinsichtlich der Verantwortung: §§ 15 Abs. 2, 16 Abs. 2 BDSG a.F.
[45] Vgl. die Forderung der DSK nach einer nachhaltigen Verantwortlichkeit aus dem Jahr 2010 *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 18.03.2010, 15 f.
[46] Vgl. etwa *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 13 f. Unzutreffend daher: *Gierschmann*, ZD 2020, 69, 69.
[47] So erkennt *Monreal*, CR 2019, 797, Rn. 2 f. große Defizite im Verständnis. Dies galt allerdings wohl unionsweit, vgl. *Korff*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 (abgerufen am 17.07.2024).

NZÖG sowie IAB Europe. Aufgrund ihrer zentralen Bedeutung für das Verständnis der gemeinsamen Verantwortlichkeit werden der Sachverhalt sowie die jeweiligen Kernaussagen dieser Urteile hier kurz dargestellt.[48]

I. Wirtschaftsakademie[49]

In der Rechtssache Wirtschaftsakademie hatte eine Stelle, die Bildungsdienstleistungen anbot (Wirtschaftsakademie) auf der Plattform eines Social Media-Plattformbetreiber (Facebook) eine spezifische Art von Benutzerkonto (Fanpage) eingerichtet, mit dem sie ihre Dienstleistungen im Rahmen der Plattform präsentieren konnte.[50] Teil des Angebots seitens des Plattformbetreibers war die Bereitstellung von anonymisierten Statistiken (Facebook Insights) über die Besucher der Fanpage. Voraussetzung für die Erstellung der Statistiken war die Erhebung von Daten der Besucher der Fanpage mittels eines Cookies, der auf den Endgeräten der Besucher gespeichert wurde.[51] Waren die Besucher bei Facebook registriert, konnte dieser Cookie mit dem Facebook-Konto verknüpft werden. Da weder der Plattformbetreiber noch der Bildungsdienstleister über die Cookies, deren Funktionsweise sowie die dazugehörige Verarbeitung informiert hatte, ging die für den Bildungsdienstleister zuständige Aufsichtsbehörde gegen diesen vor und ordnete die Deaktivierung der Fanpage an.

Der EuGH urteilte, dass der Bildungsdienstleister zusammen mit dem Plattformbetreiber gemeinsam verantwortlich sei.[52] Dabei stellte er zunächst fest, dass der Begriff des Verantwortlichen weit auszulegen sei.[53] Der Plattformbetreiber verbessere mit der fraglichen Verarbeitung sein System der Werbung, während der Bildungsdienstleister durch die Statistiken sein Marketing auf der Plattform verbessere.[54] Durch die Einrichtung einer Fanpage gebe der Bildungsdienstleister dem Plattformbetreiber die Möglichkeit, auf den Endgeräten der Besucher der Fanpage Cookies zu platzieren, unabhängig davon, ob diese Personen über ein Facebook-Konto verfügten.[55] Im Rahmen der Einrichtung der Fanpage lege der Bildungsdienstleister zudem durch „Parametrierung" die Kriterien für die Erstellung der Statistiken fest.

[48] Siehe a. die Darstellung bei: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 23 ff.

[49] Zusammengefasst: EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 2. Zum Verfahrensgang siehe a.: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 44 ff.

[50] Es handelte sich also nicht um einen normalen Nutzer der Plattform, vgl. EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 35.

[51] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 33.

[52] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 39.

[53] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 27 f.

[54] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34.

[55] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 35.

Dadurch trage der Bildungsdienstleister zur Verarbeitung seitens des Plattformbetreibers bei.[56] Die Erstellung der Statistiken wiederum beruhe auf der vorhergehenden Erhebung und Verarbeitung durch Facebook. Nötig sei schließlich auch kein Zugang zu den personenbezogenen Daten seitens aller gemeinsam Verantwortlicher, also etwa auch seitens des Bildungsdienstleisters.[57]

II. Jehovan todistajat[58]

In der Rechtssache Jehovan todistajat hatte die finnische Datenschutzaufsichtsbehörde der Gemeinschaft der Zeugen Jehovas verboten, im Rahmen der von ihren Mitgliedern von Tür zu Tür durchgeführten Verkündigungstätigkeit personenbezogene Daten zu verarbeiten, ohne dabei die datenschutzrechtlichen Voraussetzungen zu beachten. Dabei ging die Aufsichtsbehörde davon aus, dass für die Erhebung der personenbezogenen Daten im Rahmen der Verkündigungstätigkeit sowohl die Gemeinschaft als solche als auch die Mitglieder der Gemeinschaft gemeinsam verantwortlich seien.

Im Rahmen dieser Verkündigungstätigkeit machten die Mitglieder der Gemeinschaft Notizen über Besuche bei Personen, die sie aufsuchten. Zu den erhobenen Daten konnten unter anderem die Namen und Adressen der aufgesuchten Personen sowie Informationen über ihre religiösen Überzeugungen und Familienverhältnisse gehören. Diese Daten wurden als Gedächtnisstütze erhoben, ohne dass die betroffenen Personen hierin eingewilligt hätten oder hierüber informiert worden wären. Die Gemeinschaft hatte ihren Mitgliedern Anleitungen zur Anfertigung solcher Notizen gegeben, die in mindestens einem ihrer der Verkündigungstätigkeit gewidmeten Mitteilungsblätter abgedruckt waren. Die Gemeinschaft und ihre Gemeinden organisierten und koordinierten die Verkündigungstätigkeit ihrer Mitglieder insbesondere auch dadurch, dass sie Gebietskarten erstellten, auf deren Grundlage Bezirke unter den Mitgliedern, die sich an der Verkündigungstätigkeit beteiligten, aufgeteilt wurden und indem sie Verzeichnisse über die Verkündiger führten. Außerdem führten die Gemeinden der Gemeinschaft eine Liste der Personen, die darum gebeten hatten, nicht mehr von den Verkündigern aufgesucht zu werden. Die in dieser Liste enthaltenen Daten wurden von

[56] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36 ff.
[57] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 38.
[58] Zusammengefasst: EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 2. Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 56.

den Mitgliedern der Gemeinschaft verwendet. Zu einem früheren Zeitpunkt stellte die Gemeinschaft ihren Mitgliedern zudem Formulare für die Erhebung dieser Daten im Rahmen ihrer Verkündigungstätigkeit zur Verfügung. Deren Verwendung war aber zwischenzeitlich eingestellt worden.

Auch in diesem Urteil bejahte der EuGH eine gemeinsame Verantwortlichkeit, nämlich zwischen der Gemeinschaft als solcher sowie den Mitgliedern der Gemeinschaft.[59] Eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nehme und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirke, sei als Verantwortlicher anzusehen.[60] Die verkündigenden Mitglieder der Gemeinschaft würden zwar entscheiden, unter welchen konkreten Umständen sie Daten über aufgesuchte Personen erheben, welche Daten sie genau erheben und auf welche Weise sie sie anschließend verarbeiten.[61] Allerdings erfolge die Erhebung im Rahmen der Ausübung der Verkündigungstätigkeit, mit der die verkündigenden Mitglieder der Gemeinschaft den Glauben ihrer Gemeinschaft verbreiten. Diese Verkündigungstätigkeit stelle eine wesentliche Betätigungsform der Gemeinschaft dar, die von ihr organisiert und koordiniert werde und zu der sie ermuntere. In diesem Zusammenhang würden die Daten als Gedächtnisstütze zum Zweck der späteren Verwendung und für den Fall eines erneuten Besuchs erhoben. Schließlich würden die Gemeinden der Gemeinschaft auf der Grundlage der Daten, die sie von den verkündigenden Mitgliedern erhalten, Listen von Personen führen, die nicht mehr von diesen Mitgliedern aufgesucht werden möchten. Somit diene die Verarbeitung dieser Daten der Umsetzung des Ziels der Gemeinschaft, nämlich der Verbreitung ihres Glaubens, und würde folglich von ihren verkündigenden Mitgliedern im Interesse der Gemeinschaft vorgenommen. Überdies sei der Gemeinschaft der Zeugen Jehovas nicht nur bekannt, dass solche Verarbeitungen zum Zweck der Verbreitung ihres Glaubens erfolgen, sondern sie organisiere und koordiniere die Verkündigungstätigkeit ihrer Mitglieder insbesondere dadurch, dass sie die Tätigkeitsbezirke der verschiedenen Verkündiger einteile. Daraus lasse sich schließen, dass die Gemeinschaft ihre verkündigenden Mitglieder dazu ermuntere, im Rahmen ihrer Verkündigungstätigkeit personenbezogene Daten zu verarbeiten. Folglich bestünde eine gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung. Daneben hielt der EuGH

[59] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 75.
[60] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 68.
[61] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 70 ff.

zudem fest, dass eine Entscheidung über die Zwecke und Mittel der Verarbeitung nicht mittels schriftlicher Anleitungen oder Anweisungen erfolgen müsse.[62]

III. Fashion ID[63]

In der Rechtssache Fashion ID band ein Online-Händler für Modeartikel in seiner Funktion als Websitebetreiber (Fashion ID) das Social Plugin („Gefällt mir" bzw. Like-Button) eines Social Media-Plattformbetreibers (Facebook) in seine Website ein. Der Webseiten- bzw. Programmcode dieses Social Plugins sorgte bei Aufruf der Website des Websitebetreibers dafür, dass der für die Darstellung nötige Inhalt von den Servern des Plattformbetreibers abgerufen wurde. Es handelte sich dabei um eine Art Verweis.[64] Durch den Programmcode wurden also Drittinhalte in die Website des Websitebetreibers eingebunden. Rief ein Besucher die Website des Websitebetreibers auf, wurden diese Drittinhalte angefordert und zusammen mit den originären Inhalten des Websitebetreibers dargestellt. Im Rahmen dieser Anforderung wurden verschiedene, auch personenbezogene, Daten an den Server des Plattformbetreibers übermittelt. Diese Übermittlung erfolgte, ohne dass dies für den Websitebesucher erkennbar war und auch unabhängig von einer Mitgliedschaft bei der Social Media-Plattform oder vom Anklicken des Social Plugins. Um welche konkreten Daten es sich bei der Übermittlung handelte, konnte der Websitebetreiber nicht beeinflussen. Ebenso konnte er auch die weitere Verarbeitung durch den Plattformbetreiber nicht beeinflussen. Da die Websitebesucher weder in diese Verarbeitung eingewilligt hatten noch die Informationspflichten durch den Websitebetreiber oder Plattformbetreiber erfüllt wurden, ging eine deutsche Verbraucherzentrale gegen den Websitebetreiber vor.

Der EuGH stellte auch in diesem Urteil eine gemeinsame Verantwortlichkeit des Websitebetreibers und des Plattformbetreibers fest.[65] Allerdings erstrecke sich die gemeinsame Verantwortlichkeit nur auf die Verarbeitungsvorgänge, über deren Zwecke und Mittel gemeinsam entschieden würde.[66] Für eine diesen Vorgängen vor- oder nachgelagerte Verarbeitung sei nur eine zivilrechtliche Haftung nach

[62] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 67.

[63] Zusammengefasst: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 2. Zum Verfahrensgang siehe a.: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 58 ff.

[64] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 26.

[65] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 84 f.

[66] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 57.

mitgliedstaatlichem Recht denkbar. Durch die Einbindung des Social Plugins habe der Websitebetreiber die Verarbeitung ermöglicht.[67] Damit sei der Websitebetreiber aber nur für den Vorgang der Erhebung und der Übermittlung an den Plattformbetreiber gemeinsam mit diesem verantwortlich.[68] Im Rahmen der Ermöglichung bzw. Entscheidung über die Mittel habe der Websitebetreiber die Verarbeitung entscheidend beeinflusst.[69] Zwar würden Websitebetreiber und Plattformbetreiber nicht identische Zwecke verfolgen. Allerdings lägen die jeweiligen Zwecke im gegenseitigen wirtschaftlichen Interesse.[70] Der fehlende Zugang zu den verarbeiteten Daten seitens des Websitebetreibers sei unerheblich.[71] Beruhe die Verarbeitung auf dem Verarbeitungsrechtfertigungstatbestand des berechtigen Interesses, sei ein solches bei jedem der gemeinsam Verantwortlichen erforderlich.[72] Die Pflichten des gemeinsam Verantwortlichen würden sich insgesamt nur nach den Vorgängen, für die auch eine gemeinsame Verantwortlichkeit bestehe, also nicht vor- oder nachgelagerte Verarbeitungen, bemessen.[73] Allerdings sei in Fällen, in denen nur einer der gemeinsam Verantwortlichen rechtzeitig die Informationspflichten erbringen oder die Einwilligung einholen könne, nur jener dazu verpflichtet.[74] Die Reichweite der Einwilligung bzw. der Informationspflichten beschränke sich wiederum nur auf die selbst verantworteten Verarbeitungsvorgänge.

IV. NZÖG (Nacionalinis visuomenes sveikatos centras)[75]

In der Rechtssache NZÖG beauftragte der Gesundheitsminister der Republik Litauen im Zusammenhang mit der Covid-19-Pandemie den Direktor des nationalen Zentrums für Gesundheit (NZÖG) damit, den sofortigen Erwerb eines IT-Systems zur Erfassung und Überwachung der Daten der dem Virus ausgesetzten Personen zum Zweck der epidemiologischen Überwachung zu organisieren. Daraufhin teilte eine Person, die sich als Vertreter des NZÖG ausgab, einem Unternehmen (ITSS) mit, dass das NZÖG dieses Unternehmen als Entwickler einer App zur epidemiologischen Überwachung

[67] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 75.
[68] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 76.
[69] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77 ff.
[70] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80 f.
[71] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80 f.
[72] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 96 f.
[73] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 99 ff.
[74] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102 ff.
[75] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209. Hierzu a.: *Marosi*, DSB 2024, 46. Der litauische Verfahrensname lässt sich als Nationales Zentrum für öffentliche Gesundheit (NZÖG) übersetzen.

ausgewählt habe. In der weiteren Folge versandte der vermeintliche Vertreter des NZÖG E-Mails an ITSS, die sich auf verschiedene Aspekte der Entwicklung der App bezogen. Auch andere Mitarbeiter des NZÖG sandten E-Mails an ITSS, in denen es um die in der App gestellten Fragen hinsichtlich der Infektion ging. Zudem wurde eine Datenschutzerklärung für die App ausgearbeitet in der ITSS und NZÖG als Verantwortliche genannt wurden. Die App war ca. anderthalb Monate in den verschiedenen App Stores verfügbar und funktional. Eine Zustimmung zur Veröffentlichung in den App Stores gab das NZÖG weder vorab noch im Nachhinein. Während ihrer Verfügbarkeit wurden von fast viertausend Personen personenbezogene Daten über die App verarbeitet. Kurz nach Veröffentlichung der App in den App Stores beauftragte der Gesundheitsminister der Republik Litauen den Direktor des NZÖG damit den Erwerb der App von ITSS zu organisieren. Das NZÖG vergab dann allerdings keinen öffentlichen Auftrag zum offiziellen Erwerb der App von ITSS. In weiterer Folge forderte das NZÖG das Unternehmen auf, die Nennung von dem NZÖG in der App zu unterlassen. In dem auf das aufsichtsbehördliche Verfahren folgenden Gerichtsverfahren machte das NZÖG geltend, nur ITSS sei Verantwortlicher für die Verarbeitungen im Rahmen der App, während sich ITSS selbst als Auftragsverarbeiter des NZÖG verstand.

Der EuGH stellte zunächst fest, dass das NZÖG an der Entscheidung über die Zwecke und Mittel der Verarbeitung mitgewirkt habe, indem die App zur Erfassung personenbezogener Daten im Rahmen der Überwachung von Kontaktpersonen der mit dem Covid-19-Virus infizierten Personen verwendet wurde.[76] Das NZÖG habe auch aktiv an der Festlegung der Parameter der App mitgewirkt, etwa bei den in der App gestellten Fragen. Die Nennung des NZÖG in der Datenschutzerklärung der App sei allerdings nur erheblich, wenn feststünde, dass das NZÖG dem ausdrücklich oder stillschweigend zugestimmt habe.[77] Unerheblich sei auch, dass das NZÖG selbst keine personenbezogenen Daten verarbeitet habe, dass kein Vertrag zwischen dem NZÖG und ITSS bestand, dass das NZÖG die App nicht erworben habe oder dass das NZÖG der Veröffentlichung der App in den App Stores nicht zugestimmt habe.[78] Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO sei nicht nur die Stelle, die selbst personenbezogene Daten verarbeite, sondern auch die Stelle, die personenbezogene Daten in ihrem Namen verarbeiten lasse.[79] Das NZÖG könne nur dann nicht als Verantwortlicher für die Verarbeitungen, die sich aus der Veröffentlichung der App in

[76] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 32 f.
[77] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 34.
[78] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 35.
[79] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 36.

den App Stores ergeben hat, gelten, wenn es dieser Veröffentlichung ausdrücklich widersprochen hätte. Hinsichtlich der gemeinsamen Verantwortlichkeit stellte der EuGH fest, dass die Mitwirkung an der Entscheidung über die Zwecke und Mittel der Verarbeitung verschiedene Formen annehmen können. So sei denkbar, dass eine gemeinsame Entscheidung vorliege, ebenso könne aber auch eine übereinstimmende Entscheidung vorliegen. Im Falle einer übereinstimmenden Entscheidung müssten sich aber die individuellen Entscheidungen in einer Weise ergänzen, dass sich jede von ihnen konkret auf die Entscheidung über die Verarbeitungszwecke und -mittel auswirke.[80] Eine förmliche Vereinbarung über die Zwecke und Mittel der Verarbeitung sei zwischen gemeinsam Verantwortlichen nicht erforderlich.[81] Die Vereinbarung gem. Art. 26 Abs. 1 DSGVO sei Folge, nicht Voraussetzung für eine gemeinsame Verantwortlichkeit. Die Einstufung als gemeinsam Verantwortliche ergebe sich schließlich allein daraus, dass mehrere Stellen an der Entscheidung über die Zwecke und Mittel der Verarbeitung mitgewirkt hätten.

V. IAB Europe[82]

In der Rechtssache IAB Europe befasste sich der EuGH mit dem von IAB (Interactive Advertising Bureau) Europe entwickelten „Transparency & Consent Framework" (TCF). IAB Europe ist ein Verband ohne Gewinnerzielungsabsicht, der Unternehmen aus der digitalen Werbewirtschaft auf europäischer Ebene vertritt. Zu dessen Mitgliedern gehören u.a. auch Unternehmen, die durch den Verkauf von Werbeplätzen auf Websites oder in Apps Einnahmen erzielen. Der TCF stellte einen Regelungsrahmen dar, der aus Richtlinien, Anweisungen, technischen Spezifikationen, Protokollen und vertraglichen Verpflichtungen bestand. Der TCF sollte dem Anbieter einer Website oder App sowie Datenbrokern oder Werbeplattformen ermöglichen sich DSGVO-konform zu verhalten. Dies galt insbesondere, wenn diese Akteure im Rahmen des OpenRTB-Protokolls an dem Real Time Bidding teilnahmen, einem System der sofortigen und automatisierten Online-Versteigerung von Nutzerprofilen zum Handel mit Werbeplätzen im Internet.[83] Damit dem Nutzer einer Website oder App solch gezielte Werbung angezeigt werden konnte, musste vorab seine Einwilligung eingeholt werden. Bei dem ersten Aufruf der Website

[80] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 43. Der EuGH nimmt hier auf die Schlussanträge des Generalanwalts Bezug, der wiederum auf die Leitlinien des EDPB verweist.

[81] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 44 f.

[82] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328. Hierzu a.: *Halim/Marosi*, CR 2024, 297.

[83] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 22 f.

oder App erschien daher eine Einwilligungsplattform (CMP) in einem Pop-Up-Fenster, die es dem Nutzer ermöglichte, dem Anbieter der Website oder App seine Einwilligung zur Erhebung und Verarbeitung seiner personenbezogenen Daten für vorher festgelegte Zwecke (wie Marketing, Werbung oder zum Austausch mit bestimmten Anbietern) zu geben und verschiedenen Verarbeitungen, die auf der Grundlage eines berechtigten Interesses des Anbieters stattfanden, zu widersprechen. Die verarbeiteten personenbezogenen Daten betrafen insbesondere den Standort des Nutzers, sein Alter, den Verlauf seiner Suchanfragen und seine zuletzt getätigten Online-Einkäufe. Die so erfassten Präferenzen wurden dann in einen sogenannten „Transparency and Consent-String" (TC-String) kodiert und gespeichert. Dieser TC-String bestand aus einer Kombination von Buchstaben und Zeichen. Der TC-String wurde sodann mit den am OpenRTB-Protokoll beteiligten Datenbrokern geteilt. Daneben speicherte das CMP auch einen Cookie auf dem Endgerät des Nutzers, der zusammen mit dem TC-String der IP-Adresse des Nutzers zugeordnet werden konnte. Im Rahmen des aufsichtsbehördlichen Verfahrens entschied die zuständige belgische Aufsichtsbehörde, dass IAB Europe Verantwortlicher sei, u.a. hiergegen wehrte sich IAB Europe dann gerichtlich.

Der EuGH bestätigte die Auffassung der belgischen Aufsichtsbehörde, dass IAB Europe zusammen mit allen seinen Mitgliedern gemeinsam Verantwortlicher hinsichtlich der Verarbeitungen im Rahmen des TCF sei. Dass es sich bei dem TCF nicht nur um eine technische Spezifikation oder Norm handelte, war bereits durch die Vorlagefragen vorgegeben.[84] Die Entscheidung enthält inhaltlich wenig Neues gegenüber den vorherigen Entscheidungen zur gemeinsamen Verantwortlichkeit. Sie stellt die bisherige Rechtsprechung überblicksartig dar,[85] und vertieft die Rechtsprechung aus der Rechtssache Jehovan todistajat im Hinblick auf die gemeinsame Verantwortlichkeit einer Institution und seiner Mitglieder. IAB Europe habe im Interesse der Ermöglichung und Förderung des Handels mit Werbeplätzen im Internet für seine Mitglieder den TCF entwickelt und damit gemeinsam mit den Mitgliedern den Zweck der Verarbeitung festgelegt.[86] Hinsichtlich der Entscheidung über die Mittel stellte der EuGH fest, dass sich die Mitglieder an die Vorgaben aus dem TCF halten müssen, wenn sie dem Verband beitreten.[87] IAB Europe könne Mitglieder, die sich nicht an den TCF halten hiervon suspendieren und schließlich ausschließen. Daneben enthalte der TCF technische Spezifikationen für die Verarbeitung des TC-

[84] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 31.
[85] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 54 ff.
[86] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 62 ff.
[87] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 65.

Strings, etwa wie die Präferenzen der Nutzer zu sammeln und wie der TC-String zu generieren sei.[88] Ebenso gebe es auch Regeln für die Speicherung und den Austausch des TC-Strings. Schließlich schreibe IAB Europe auf standardisierte Art und Weise vor, wie die am TCF beteiligten Parteien die im TC-String enthaltenen Präferenzen, Widersprüche und Einwilligungen der Nutzer einsehen könnten.[89] Weiter merkte der EuGH an, dass der fehlende unmittelbare Zugang von IAB Europe zum TC-String unerheblich sei für die Feststellung der gemeinsamen Verantwortlichkeit.[90] Hinsichtlich der Reichweite der Verantwortlichkeit stellte der EuGH fest, dass IAB Europe nur für die Verarbeitungen im Rahmen des TCF gemeinsam Verantwortlicher sei, allerdings nicht für die weitere Verarbeitung aufgrund der Präferenzen aus dem TC-String.[91]

C. Vorfragen - „Gemeinsam“ im Kontext der Definition

Für eine Analyse des Definitionselements „gemeinsam“ muss dieses im Kontext der Definition des Verantwortlichen betrachtet werden. Dabei stellt sich zunächst die Frage, ob es verschiedene Definitionen der gemeinsamen Verantwortlichkeit in der DSGVO gibt. Neben dem unmittelbaren Kontext des Definitionselements „gemeinsam“ ist auch sein Bezugsobjekt innerhalb der Definition erheblich. Schließlich stellt sich die Frage, ob die gemeinsam Verantwortlichen neben oder statt ihrer individuellen Verantwortlichkeit ein Rechtssubjekt sui generis darstellen. Es stellt sich also die Frage, ob die gemeinsame Verantwortlichkeit eine eigene „Zuordnungsmasse“ für Pflichten und Haftung darstellt. Dies ist auch im Hinblick auf das Erfordernis einer Verarbeitungsrechtfertigung zwischen den gemeinsam Verantwortlichen erheblich.

Der Duden definiert „gemeinsam“ unter anderem als „in Gemeinschaft [unternommen, zu bewältigen]; zusammen, miteinander“.[92] „Gemeinsam“ bezeichnet also eine Handlung, die in Personenmehrheit vorgenommen wird. Ausgehend von einer reinen Wortlautauslegung deutet das „gemeinsam“ also schlicht darauf hin, dass an der Entscheidung nicht nur ein Akteur beteiligt ist.

[88] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 66.
[89] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 67.
[90] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 69.
[91] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 74 f.
[92] https://www.duden.de/rechtschreibung/gemeinsam (abgerufen am 17.07.2024).

I. Art. 4 Nr. 7 vs. Art. 26 Abs. 1 S. 1 DSGVO – unterschiedliche Definitionen der gemeinsam Verantwortlichen?

Aufgrund der nicht wortgleichen Definitionen in Art. 4 Nr. 7 DSGVO („die [...] Stelle die [...] gemeinsam mit anderen [...]“) und Art. 26 Abs. 1 S. 1 DSGVO[93] („[...] so sind sie gemeinsam Verantwortliche.“) könnte man annehmen, dass es sich bei den definierten Akteuren jeweils um unterschiedliche Rechtsfiguren handelt.[94] So spricht Art. 4 Nr. 7 DSGVO von „entscheiden“, wohingegen Art. 26 Abs. 1 S. 1 DSGVO das Verb „festlegen“[95] verwendet. Diese Diskrepanz ist allerdings den Änderungen im Gesetzgebungsverfahren[96] sowie der Übersetzung geschuldet. Dies zeigt ein Vergleich mit der englischen und französischen Version der DSGVO.[97] Neben den unterschiedlichen Verben könnte man der Definition in Art. 26 Abs. 1 S. 1 DSGVO auch entnehmen, dass für gemeinsam Verantwortliche bereits eine Verantwortlichkeit bestehen muss („Legen zwei oder mehr Verantwortliche [...] so sind sie gemeinsam Verantwortliche“).[98] Hierbei ist Art. 26 Abs. 1 S. 1 DSGVO letztlich nur präziser, da Art. 4 Nr. 7 DSGVO (rein grammatikalisch) sowohl den einzelnen als auch die gemeinsam Verantwortlichen definiert. Bei Art. 4 Nr. 7 DSGVO und Art. 26 Abs. 1 S. 1 DSGVO handelt es sich also um dieselbe Rechtsfigur der gemeinsam Verantwortlichen.[99]

II. Unmittelbarer Kontext: „mit anderen“

Ausgehend vom Wortlaut der Definition in Art. 4 Nr. 7 DSGVO bildet das Definitionselement „gemeinsam“ den Gegenpart zu „allein“. Dabei heißt es „gemeinsam mit anderen“. Eine weitere Qualifizierung des Elementes „gemeinsam“ erfolgt nicht. Es könnte also theoretisch jedes (Rechts-)Subjekt durch „mit anderen“ gemeint sein. Dies gilt insbesondere dann, wenn man das „mit anderen“ auf die vorher

[93] Vgl. Art. 21 DSRL-JI.

[94] *Monreal*, CR 2019, 797, Rn. 6. Unschön dargestellt bei: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 7, 13 f.

[95] Dabei könnte man „festlegen“ im Vergleich zu „entscheiden“ als finaleren Schritt verstehen, so: *Monreal*, CR 2019, 797, Rn. 9.

[96] Die Definition in Art. 26 Abs. 1 S. 1 DSGVO wurde erst durch den Rat eingebracht: DSGVO-E (Rat) v. 11.06.2015, 9565/15, S. 111.

[97] „(Jointly) determine“ bzw. „détermine“ in beiden Normen.

[98] *Monreal*, CR 2019, 797, Rn. 8.

[99] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 51; vgl. a. Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 5; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 11.

aufgezählten Organisationseinheiten und deren Oberbegriff der „Stelle“ bezieht.[100] Allein wegen Art. 29 DSGVO, der die dem Verantwortlichen unterstellten Personen hinsichtlich der Verarbeitung privilegiert, muss aber ein vom Verantwortlichen abgrenzbares Rechtssubjekt vorliegen. Denn die dem Verantwortlichen unterstellten Personen verarbeiten nur auf dessen Weisung. Sie können also logischerweise nicht mit ihm gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden. Daher muss für die Abgrenzung anderer Rechtssubjekte auf die Definition des Dritten in Art. 4 Nr. 10 DSGVO zurückgegriffen werden.[101] Die „anderen“ im Rahmen der Definition des Verantwortlichen sind also von dem jeweiligen Verantwortlichen ausgehend bestimmte „Dritte“ gem. der Definition in Art. 4 Nr. 10 DSGVO.[102] Diese sind „eine [...] andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;“. Die DSGVO bestimmt den Begriff des Dritten negativ. Erfüllt ein Akteur, relativ zum maßgeblichen Verantwortlichen, keine dieser Rollen, ist er ein Dritter. Von diesen Dritten kann aber wiederum nur ein anderer Verantwortlicher das Kriterium von „mit anderen“ i.S.v. Art. 4 Nr. 7 DSGVO erfüllen, da Art. 26 Abs. 1 S. 1 DSGVO ausdrücklich „zwei oder mehr Verantwortliche“ voraussetzt. Daneben wird auch in Art. 4 Nr. 7 DSGVO anhand des Definitionsteils „gemeinsam mit anderen [...] entscheidet“ klar, dass es sich bei den „anderen“ nur um solche Akteure handeln kann, die eine gewisse Entscheidungsmacht besitzen. Ein Auftragsverarbeiter kann schon mangels hinreichender Entscheidungsmacht nicht unter die „anderen“ fallen. „Gemeinsam mit anderen“ setzt also neben dem maßgeblichen Verantwortlichen mindestens einen weiteren Verantwortlichen voraus, der relativ zu diesem Dritter ist.[103] Diese Verantwortlichen werden erst durch die gemeinsame Entscheidung überhaupt zu Verantwortlichen. Sie müssen trotz des missverständlichen Wortlautes in Art. 26 Abs. 1 S. 1 DSGVO nicht unabhängig von der konkreten gemeinsamen Entscheidung bereits Verantwortliche sein.[104] Auch wenn der Wortlaut des Art. 4 Nr. 7 DSGVO hinsichtlich der Mindestmenge an Akteuren bei einer gemeinsamen

[100] Dazu: Kapitel 2 B. Stelle.

[101] Ein Rückgriff auf den Definitionsteil „andere Stelle“ wäre hingegen zirkulär.

[102] Dazu: Kapitel 1 A. I. Relevante Akteure für die Verantwortlichkeit; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 89; vgl. *Piltz*, https://www.delegedata.de/2020/10/der-dritte-nach-der-dsgvo/ (abgerufen am 17.07.2024).

[103] Kritisch S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 18, 44, der darauf hinweist, dass die gemeinsam Verantwortlichen nicht a. separat Verantwortliche sein müssten. Dies gelte insbesondere im Hinblick auf den fehlenden Zugang zu den Daten.

[104] Klarstellend: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 24.

Verantwortlichkeit bereits hinreichend deutlich sein sollte („gemeinsam mit anderen"),[105] stellt die Definition des Art. 26 Abs. 1 S. 1 DSGVO noch einmal klar, dass bereits zwei Verantwortliche gemeinsam Verantwortliche bilden können.[106] Nach oben ist die Grenze der beteiligten Verantwortlichen theoretisch offen. Aufgrund der Beteiligung weiterer individueller Verantwortlicher lässt sich das Definitionselement „gemeinsam" deswegen insgesamt auch schlicht als „nicht allein" lesen.[107]

III. Bezugsobjekt: „entscheidet"

Ein neuralgischer Punkt des Definitionselements „gemeinsam" ist dessen Bezugsobjekt. So gehen Teile der Literatur davon aus, dass zumindest ein gemeinsamer Zweck bei gemeinsam Verantwortlichen erforderlich sei.[108] Demnach wird „gemeinsam" also auf die Zwecke, teilweise auch auf die Mittel, bezogen.[109] Rein grammatikalisch ist das Bezugsobjekt von „gemeinsam" aber das Wort „entscheidet".[110] Dies wird deutlich durch den Einschub „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten". Dieser Einschub definiert worüber entschieden wird. Er hat allerdings nichts mit dem Element „gemeinsam" zu tun. Somit sind, jedenfalls ausgehend von dem Wortlaut, gemeinsame Zwecke und/oder Mittel nicht zwingend erforderlich.[111] Eine gemeinsame Entscheidung über diese Zwecke und Mittel der Verarbeitung ist hingegen sehr wohl erforderlich. Auch in Art. 26 Abs. 1 S. 1 DSGVO ist der Wortlaut insoweit eindeutig: „legen zwei oder mehr Verantwortliche gemeinsam [...] fest". Alle gemeinsam Verantwortlichen müssen also einen Entscheidungsbeitrag leisten.[112]

Maßgebliches Kriterium für die gemeinsame Entscheidung ist also rein grammatikalisch die Entscheidungsautonomie der beteiligten Akteure.[113] Da sich Kollaborationsszenarien vor allem dann anbieten, wenn ein Verantwortlicher eine Verarbeitung mangels entsprechender Mittel oder Expertise nicht allein durchführen

[105] Denkbar wäre der – zugegebenermaßen spitzfindige – Einwand der Plural in „anderen" in Art. 4 Nr. 7 DSGVO würde mindestens zwei weitere Verantwortliche (also insgesamt mindestens drei) implizieren. Gleichermaßen ließe sich bei einer Formulierung wie „mit einem anderem" einwenden, es dürften nicht mehr als zwei Verantwortliche gemeinsam verantwortlich sein.

[106] Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 24.

[107] Vgl. Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 2.

[108] *Moos/Rothkegel*, MMR 2019, 584, 585.

[109] Siehe dazu die folgenden Ausführungen.

[110] So a.: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 24.

[111] Dazu: Kapitel 4 H. III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung.

[112] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 31.

[113] Dazu: Kapitel 4 J. Indizien für eine Abgrenzung zum Auftragsverarbeiter.

kann, liegt es nahe, dass gemeinsam Verantwortliche häufig arbeitsteilig handeln.[114] Diese Arbeitsteilung kann sich sowohl auf eine Teilentscheidung[115] innerhalb der Zwecke und/oder der Mittel als auch auf die Entscheidung über die Zwecke und Mittel insgesamt[116] erstrecken. Ausgehend vom Wortlaut ist nur das Ergebnis, eine (gemeinsame) Entscheidung insgesamt über die Zwecke und Mittel der Verarbeitung zwingend.[117] Auch nach Ansicht der Art. 29-Datenschutzgruppe kann durch das Merkmal „gemeinsam“ eine Vielzahl verschiedenster Kollaborationsszenarien erfasst werden, nicht nur eine paritätische Gesamtentscheidung[118] der gemeinsam Verantwortlichen.

IV. Gemeinsam Verantwortliche als Rechtssubjekt sui generis?

Aufgrund des Wortlautes in Art. 26 Abs. 1 S. 1 DSGVO („[...] so sind sie gemeinsam Verantwortliche.“) könnte man annehmen, bei gemeinsam Verantwortlichen handelt es sich um ein gegenüber den individuell beteiligten Verantwortlichen selbstständiges Rechtssubjekt. Wenn man diesem Gedanken folgt, bestünde, vergleichbar mit der Haftung bestimmter Gesellschaftsformen im Gesellschaftsrecht, abseits oder statt der beteiligten Verantwortlichen noch eine Art „gemeinsame Verantwortlichkeitsmasse“. Im Zusammenhang mit einer solchen „gemeinsamen Verantwortlichkeitsmasse“ wäre es fraglich, ob noch eine Verarbeitungsrechtfertigung für eine Übermittlung innerhalb dieser „gemeinsamen Verantwortlichkeitsmasse“, also für die gemeinsam verantworteten Verarbeitungsvorgänge, notwendig wäre.[119] Denn soweit die individuell beteiligten Verantwortlichen Teil der „Verantwortlichkeitsmasse“ wären oder im Hinblick auf die gemeinsame Verantwortlichkeit nur die „Verantwortlichkeitsmasse“ überhaupt bestünde, würde kein Dritter vorliegen. Die gemeinsam Verantwortlichen wären alle Teil einer identischen „Verantwortlichkeitsmasse“, also einer Stelle im Sinne der Definition. Im

[114] *Kremer*, CR 2019, 225, Rn. 18.

[115] Alle Verantwortlichen entscheiden sowohl über Zwecke als auch Mittel maßgeblich mit. Dies wäre ein prozessbezogenes Verständnis von „gemeinsam entscheiden“.

[116] Ein Verantwortlicher entscheidet etwa über die Zwecke, ein anderer über die Mittel. Dies wäre ein ergebnisbezogenes Verständnis von „gemeinsam entscheiden“.

[117] Dazu: Kapitel 4 H. III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung.

[118] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22. Dabei sei darauf hingewiesen, dass die dort referenzierte Stellungnahme der Kommission aus dem Jahre 1995 (COM/95/0375 FINAL - COD 287) stammt, das WP 169 der Art. 29-Datenschutzgruppe hingegen aus dem Jahr 2010. In diesen 15 Jahren gab es natürlich eine erhebliche technische Entwicklung.

[119] Dazu: Kapitel 4 L. I. Privilegierung der Übermittlung zwischen gemeinsam Verantwortlichen?

erstgenannten Fall (Verantwortliche als Teil einer „Verantwortlichkeitsmasse“) wäre zwar noch eine Übermittlung der individuell beteiligten Verantwortlichen an die „Verantwortlichkeitsmasse“ denkbar. Allerdings wäre völlig unklar, wie diese Übermittlung von anderen Übermittlungen innerhalb des individuell beteiligten Verantwortlichen abzugrenzen wäre.

Hinsichtlich einer „gemeinsamen Verantwortlichkeitsmasse“ lässt sich zunächst festhalten, dass Art. 4 Nr. 7 DSGVO zwei Varianten der Verantwortlichkeit kennt, die singuläre – der Verantwortliche entscheidet allein – sowie die pluralistische[120] – der Verantwortliche entscheidet gemeinsam mit anderen. Dabei bedeutet „gemeinsam“, wie bereits dargestellt, „nicht allein“.[121] Sofern Art. 4 Nr. 7 DSGVO und Art. 26 Abs. 1 S. 1 DSGVO dieselbe gemeinsame Verantwortlichkeit definieren, finden sich in Art. 4 Nr. 7 DSGVO keinerlei Hinweise für ein weiteres Rechtssubjekt. Denn dort heißt es explizit: „[...] gemeinsam mit anderen [...] entscheidet;“. Auch in Art. 26 Abs. 1 S. 1 DSGVO finden sich keine expliziten Hinweise auf ein weiteres Rechtssubjekt, es heißt dort: „Legen zwei oder mehr Verantwortliche gemeinsam [...] fest [...]“. Diese Verantwortlichen zeichnen sich also durch ein kollaboratives Element aus.[122] „Gemeinsam Verantwortliche“ ist dabei schlicht die Bezeichnung für diese Variante der Verantwortlichkeit. Bestünde eine einheitliche „gemeinsame Verantwortlichkeitsmasse“, wären etwa die Erleichterungen für die betroffene Person hinsichtlich des Schadensersatzes (Art. 82 Abs. 4 DSGVO) oder der Betroffenenrechte (Art. 26 Abs. 3 DSGVO) nicht notwendig. Dass kein weiteres Rechtssubjekt im Rahmen der gemeinsamen Verantwortlichkeit beabsichtigt war, deckt sich auch mit der Genese von Art. 26 DSGVO. Eine Privilegierung der gemeinsam Verantwortlichen wurde zwar erörtert, letztlich aber verworfen.[123] Eine solche Privilegierung der einzelnen Akteure hinsichtlich einens Schadensersatzes oder als Adressat der Betroffenenrechte wäre aber nicht möglich gewesen, wenn sie ohnehin eine einheitliche

[120] Diesen Begriff verwendet die Art. 29-Datenschutzgruppe: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 10.

[121] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 51; *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 504; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 25; *Monreal*, CR 2019, 797, Rn. 40.

[122] Falsch erscheint daher die Prämisse von *Hacker*, MMR 2018, 779, 780, dass sich gemeinsame Verantwortlichkeit nicht nur aus tatsächlicher Kontrolle, sondern auch aus fehlender Transparenz ergeben kann. Dies beruht wohl auf einem fehlerhaften Grundverständnis, wann ein hinreichender Beitrag eines (potenziell) gemeinsam Verantwortlichen vorliegt.

[123] G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 29 ff.

„gemeinsame Verantwortlichkeitsmasse“ bilden würden. Die gemeinsam Verantwortlichen in Art. 26 Abs. 1 S. 1 DSGVO sind also gerade kein neues Rechtssubjekt sui generis.[124]

Auch eine Analyse der jüngeren Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit führt zu keinem anderen Ergebnis. Die gemeinsame Verantwortlichkeit drückt nur eine gewisse Verbundenheit von grundsätzlich individuellen Verantwortlichen aus. Deutlich wird dies etwa in der Rechtssache Wirtschaftsakademie.[125] Dort formuliert der EUGH: „[...] wobei dann jeder von ihnen [den gemeinsam Verantwortlichen] den Datenschutzvorschriften unterliegt“.[126] Genau diese Formulierung greift der EuGH dann in den Rechtssachen Jehovan todistajat[127] und Fashion ID[128] wieder auf. Insofern ist hier von einer gefestigten Rechtsprechung auszugehen.[129] Deutlich macht der EuGH zudem auch, dass für jeden individuellen gemeinsam Verantwortlichen jeweils ein, möglicherweise aber auch identischer, Verarbeitungsrechtfertigungstatbestand vorliegen muss.[130] Würde die gemeinsame Verantwortlichkeit ein neues Rechtssubjekt schaffen, wäre ein individueller Verarbeitungsrechtfertigungstatbestand gerade nicht notwendig.[131]

Der EuGH hatte in der Rechtssache Fashion ID zwar die Einholung einer Einwilligung für beide gemeinsam Verantwortliche durch einen der gemeinsam Verantwortlichen für möglich erachtet.[132] Diesem lag aber der Sachverhalt zugrunde, dass eine Verarbeitung der personenbezogenen Daten eines Websitebesuchers bereits bei dessen Aufruf der Website des Websitebetreibers erfolgte. Eine Interaktionsmöglichkeit des Websitebesuchers mit dem Plattformbetreiber, der dessen Daten aufgrund eines Social Plugins innerhalb der Website des Websitebetreibers verarbeitete, war nicht gegeben. Die Einholung der Einwilligung durch den Websitebetreiber auch für den Plattformbetreiber stellte insofern einen Sonderfall dar,

[124] *Monreal*, CR 2019, 797, Rn. 12; nicht nachvollziehbar ist daher, inwiefern eine Auftragsverarbeitung durch gemeinsam Verantwortliche zusammen veranlasst werden könnte: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 68; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 15.

[125] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[126] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 29; *Kollmar*, NVwZ 2019, 1740, 1742; *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 33.

[127] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 65.

[128] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 67.

[129] So a. *Kremer*, CR 2019, 676, Rn. 17 und *Golland*, K&R 2019, 533, 534 mit Verweis auf die Rechtssache Fashion ID.

[130] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 96.

[131] *Monreal*, CR 2019, 797, Rn. 54.

[132] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, 102 ff.

der durch die rechtzeitige Information der betroffenen Person bedingt war.[133] Daneben war diese Einholung der Einwilligung in ihrer Reichweite allerdings auch insoweit beschränkt, wie der Websitebetreiber selbst an den Verarbeitungsvorgängen als gemeinsam Verantwortlicher beteiligt war.[134] Für weitere Verarbeitungsvorgänge musste der andere gemeinsam Verantwortliche, in diesem Fall der Plattformbetreiber, also selbst den Informationspflichten nachkommen und eine weitere Einwilligung einholen.

D. Die Verarbeitung als Vorgangsreihe bei gemeinsam Verantwortlichen

Maßgeblich für die Bestimmung der Verantwortlichkeit ist das Bezugsobjekt der Entscheidung, die Verarbeitung. Wie bereits dargestellt,[135] kann eine Verarbeitung sowohl aus einzelnen Vorgängen wie auch Vorgangsreihen bestehen. Die Verklammerung einzelner Vorgänge zu einer Vorgangsreihe erfolgt dabei durch einen übergreifenden Zweck.[136] Für gemeinsam Verantwortliche ist die Vorgangsreihe dahingehend relevant, dass sie die Reichweite der individuellen Verantwortlichkeit eines gemeinsam Verantwortlichen bestimmen kann, also für welche konkreten Vorgänge er gemeinsam verantwortlich ist.

I. Divergierende Zwecke

Wenn der jeweilige Zweck[137] bei gemeinsam Verantwortlichen nicht in einem gemeinsamen Zweck, sondern in divergierenden Zwecken besteht,[138] können entsprechend der Verklammerungswirkung des jeweiligen Zweckes auch die Vorgangsreihen zwischen den gemeinsam Verantwortlichen divergieren und somit

[133] Dazu: Kapitel 4 L. V. Delegation von Pflichten zwischen gemeinsam Verantwortlichen; EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102; deutlich: EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 132.

[134] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[135] Dazu: Kapitel 2 A. Bezug zur Verarbeitung.

[136] Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 118 f. Wohl a.: *Gierschmann*, ZD 2020, 69, 71.

[137] Bzw. die Zwecke. Der Verständlichkeit halber wird hier aber jeweils ein einzelner Zweck der Verantwortlichen angenommen.

[138] Dementsprechend müsste für eine gemeinsame Verantwortlichkeit allerdings noch ein gemeinsames Mittel bestehen: Kapitel 4 H. II. Gemeinsame Zwecke oder Mittel als Identitätsgarant der Verarbeitung.

unterschiedliche einzelne Vorgänge erfassen.[139] Anders ausgedrückt: Vorgangsreihen bestehen relativ zum gemeinsam Verantwortlichen, nicht insgesamt für die gemeinsam Verantwortlichen. Für die Zwecke des einen gemeinsam Verantwortlichen mag ein einzelner Vorgang im Rahmen einer Vorgangsreihe notwendige Voraussetzung sein, für den anderen nicht.

Illustrativ hierfür ist das Urteil des EuGH in der Rechtssache Wirtschaftsakademie.[140] Der EuGH stellte dort fest, dass ein Bildungsdienstleister, der eine Seite auf einer Social Media-Plattform eingerichtet hatte, nicht nur einen generellen Vermarktungszweck verfolgte, sondern vom Plattformbetreiber auch Statistiken über seine Besucher begehrte.[141] Für die Erstellung der Statistiken konnte der Bildungsdienstleister die Seite bei der Plattform entsprechend einrichten bzw. parametrieren.[142] Der Bildungsdienstleister erhielt die vom Plattformbetreiber erhobenen und analysierten Daten dann in einer anonymisierten Statistik zurück. Die Erhebung dieser Daten wiederum wurde durch die Einrichtung der Seite ermöglicht. Denn beim Abruf der Seite wurde ein Cookie auf den Endgeräten der Besucher dieses Informationsangebots des Bildungsdienstleisters gesetzt.[143]

Dabei stellt die Erhebung der Daten der Seitenbesucher durch den Plattformbetreiber für diesen einen separaten Vorgang dar, der nicht unbedingt mit der Erstellung der Statistik zusammenhängen musste. So könnte für den Plattformbetreiber ein die Verarbeitungsvorgänge übergreifender Zweck etwa in der Schaltung von Werbung bestehen. Von diesem Zweck wären dann andere einzelne Vorgänge erfasst als für die Erstellung der Statistik. Für den Bildungsdienstleister hingegen stellt der Vorgang der Erhebung der Daten, als notwendige Vorbedingung, und die Verarbeitung zu einer Statistik, nach den Vorgaben der Parametrierung, aufgrund des verbindenden Zweckes der Erstellung der Statistik eine einheitliche Vorgangsreihe dar.[144] Deutlich wird hierbei, dass es bei gemeinsam Verantwortlichen kritisch ist die jeweiligen Zwecke präzise zu bestimmen, um dann die Reichweite[145]

[139] In diese Richtung wohl: Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 23. Ähnlich a. Taeger/Gabel/*Gabel/Lutz*, Art. 28 DSGVO, Rn. 20 zu Auftragsverarbeitern. Möglicherweise lässt sich a. EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70 so verstehen. Ebenso: *Monreal*, CR 2019, 797, Rn. 35.

[140] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[141] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34.

[142] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36 f.

[143] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 38.

[144] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 38.

[145] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

ihrer jeweiligen Verantwortlichkeit anhand der für sie relevanten Vorgänge bzw. Vorgangsreihen festzulegen.

II. Gemeinsame Zwecke

Sofern bei der Verarbeitung durch gemeinsam Verantwortliche ein gemeinsamer Zweck[146] vorliegt, kann über diesen Zweck eine einheitliche Vorgangsreihe für alle beteiligten Verantwortlichen bestehen. In diesem Fall wäre die Vorgangsreihe also nicht nur für einen der gemeinsam Verantwortlichen individuell maßgeblich. Ebenso kann dann eine einheitliche Vorgangsreihe für gemeinsam Verantwortliche bestehen, wenn diese zur Erreichung des Zweckes der Vorgangsreihe zwar jeweils unterschiedliche Verarbeitungsvorgänge mit den Daten vornehmen, insoweit aber voneinander abhängig sind.[147] Auch für Vorgangsreihen, nicht nur für einzelne Vorgänge, kann also ein gemeinsamer Zweck vorliegen.[148]

Illustrativ hierfür ist das Beispiel 10 in WP 169.[149] In diesem Beispiel setzte eine Bank zur Durchführung einer Finanztransaktion einen Übermittler von Finanzmitteilungen ein. Bank und Übermittler einigten sich zwar auf die Mittel für die Verarbeitung der Finanzdaten, die Verarbeitung selbst erfolgte dabei aber in verschiedenen Phasen teils durch die Bank und teils durch den Übermittler. Die Zwecke der Bank und des Übermittlers waren auf der Mikroebene[150] der verschiedenen Phasen bzw. Vorgänge zwar nicht identisch, dienten aber auf der Makroebene[151] der Vorgangsreihe der Durchführung der Finanztransaktion.[152] Entgegen den Ausführungen der Art. 29-Datenschutzgruppe in WP 169[153] entstand durch die Verwendung gemeinsamer Mittel aber nicht eine weitere Makroebene vergleichbar zur Vorgangsreihe (aufgrund des Zweckes). Allein die Entscheidung über gemeinsame Mittel verbindet verschiedene Vorgänge noch nicht zu einer Vorgangsreihe.

---

[146] Also nicht nur eine Zweckkomplementarität.

[147] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 43.

[148] Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 13.

[149] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 25.

[150] Die genauen Zwecke führt das WP 169 nicht weiter aus.

[151] Vgl. zum Begriff Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 13.

[152] Hat Verantwortlicher A für Vorgang X Zweck 1 und Verantwortlicher B für Vorgang Y Zweck 2 könnte ein Zweck der Vorgangsreihe XY im Sinne von 12 gebildet werden.

[153] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 25.

III. Möglicher Abstraktionsgrad der Zwecke

Der Zweck einer Verarbeitung kann nicht beliebig weit abstrahiert werden, um noch eine Vorgangsreihe bilden zu können. Denn dies würde mit dem Zweckbindungsgrundsatz[154] aus Art. 5 Abs. 1 lit. b DSGVO im Konflikt stehen. Verschiedene Vorgänge können als Vorgangsreihe nur verklammert werden, soweit dies für einen hinreichend präzisen Zweck nötig ist.[155] Mit anderen Worten: die Grenze der Zweckabstraktion im Rahmen einer Vorgangsreihe ist der Zweckbindungsgrundsatz. Die Außenperspektive, etwa von betroffenen Personen, auf den vermeintlichen Zweck ist nicht maßgeblich, da die Festlegung der Zwecke durch die Verantwortlichen erfolgt.[156] Umgekehrt kann und muss der Zweck einer Vorgangsreihe auf die einzelnen Vorgänge gespiegelt werden, sofern für diese keine konkreten Zwecke festgelegt wurden.

IV. Verhältnis zur Zweckkomplementarität

Abzugrenzen ist die Makroebene der Vorgangsreihe von der Makroebene der Zweckkomplementarität.[157] Die Makroebene der Zweckkomplementarität bezieht sich auf die Vereinbarkeit divergierender Zwecke zwischen gemeinsam Verantwortlichen. Hierfür reicht bereits ein einzelner Verarbeitungsvorgang aus. Eine gemeinsame Vorgangsreihe hingegen kann nur dann gebildet werden, wenn zwischen den gemeinsam Verantwortlichen mehrere Vorgänge vorliegen und somit abstrahiert werden können. Einfach ausgedrückt: Verfolgen zwei Verantwortliche für denselben Vorgang unterschiedliche Zwecke liegt weiterhin nur ein Verarbeitungsvorgang vor.[158] Mangels mehrerer Verarbeitungsvorgänge kann dann keine Vorgangsreihe gebildet

[154] Präziser mit dem Zweckfestlegungsgrundsatz als Aspekt der Zweckbindung.

[155] Vgl. *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, ²2012, Rn. 123 ff.; vgl. a. *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, ³2022, Rn. 83.

[156] Insofern geht die Kritik bei *Kartheuser/Nabulsi*, MMR 2018, 717, 719 zu dem Reisebüro-Beispiel des WP 169 und dem übergeordneten Zweck „Reise" fehl.

[157] Dazu gleich unter: Kapitel 4 E. I. 6. „Interesse" als Zweckkomplementarität. Falsch liegen daher wohl *Lezzi/Oberlin*, ZD 2018, 398, 400, die argumentieren, dass die Makroebene der Datenverarbeitung in Betracht gezogen werden müsse, a. wenn auf der Mikroebene gemeinsam Verantwortliche eigene Zwecke verfolgen.

[158] Also Verantwortlicher A verfolgt für Vorgang X Zweck 1 und Verantwortlicher B verfolgt für Vorgang X Zweck 2.

werden. Eine Zweckkomplementarität könnte hingegen auch bei nur einem Verarbeitungsvorgang durchaus vorliegen.

Verfolgt etwa ein Verein mit einer Mitgliederbefragung Zwecke der Meinungsbildung, ein daran beteiligter Wissenschaftler hingegen mit bestimmten Fragen Forschungszwecke, kann bei einer gemeinsamen Erhebung Zweckkomplementarität vorliegen, eine Vorgangsreihe liegt allerdings nicht vor. Lässt hingegen der Verein die Mitgliederbefragung durch den Wissenschaftler durchführen, können die Erhebung, Auswertung und die Übermittlung des Ergebnisses für den Verein eine Vorgangsreihe unter dem Zweck der Mitgliederbefragung darstellen.

E. Die Zwecke der Verarbeitung als Entscheidungsobjekt

Obwohl das grammatikalische Bezugsobjekt von „gemeinsam" in der Definition der gemeinsam Verantwortlichen „entscheiden" bzw. „festlegen" ist (so in Art. 4 Nr. 7 DSGVO: „die [...] Stelle, die [...] **gemeinsam** mit anderen [über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten] **entscheidet**"), setzt ein Teil der Literatur darüber hinaus einen gemeinsamen Zweck der Verantwortlichen voraus.[159] Es wird demnach neben einer gemeinsamen Entscheidung ein gemeinsamer Zweck gefordert. Näher begründet wird diese vermeintliche, zusätzliche Voraussetzung nicht. Der Reiz der vermeintlichen Notwendigkeit eines gemeinsamen Zweckes scheint darin zu liegen, dass eine gemeinsame Verantwortlichkeit einfacher erkennbar und gleichzeitig in ihrem Anwendungsbereich eingeschränkt wird. Ob der EuGH aber einen solchen gemeinsamen Zweck tatsächlich voraussetzt oder ob schon eine Zweckkomplementarität ausreicht, soll hier näher untersucht werden.

I. *Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen*

1. Das Urteil und die Schlussanträge zu Fashion ID

Anlass für eine tiefere Analyse des Definitionselements des Zweckes in Bezug auf gemeinsam Verantwortliche bietet das Urteil des EuGH in der Rechtssache Fashion ID[160]. Versteht man die Entscheidung über die Zwecke als wesentlich für die

[159] So etwa: *Moos/Rothkegel*, MMR 2019, 584, 585; *Lee/Cross*, MMR 2019, 559, 562. Unklar: *Golland*, K&R 2019, 533, 535.

[160] Dazu: Kapitel 4 B. III. Fashion ID.

Einordnung als Verantwortlicher,[161] fallen die Ausführungen des EuGH in der Rechtssache Fashion ID mit einer Randnummer äußerst knapp aus.[162] So hielt der EuGH fest, dass der Websitebetreiber zwecks Optimierung der Werbung für seine Produkte das Social Plugin des Plattformbetreibers in seine Website einband und dadurch auch in die damit verbundene Datenerhebung des Plattformbetreibers einwilligte[163]. Der Plattformbetreiber wiederum stelle das Social Plugin zur Verfügung, um die damit erhobenen personenbezogenen Daten für eigene wirtschaftliche Zwecke zu erlangen.[164] Zweck des Vorgangs der Datenerhebung durch das Social Plugin schien also für den Websitebetreiber die optimierte Werbung zu sein, für den Plattformbetreiber die uneingeschränkte Verfügung über die Daten für eigene wirtschaftliche Zwecke. Beide Akteure verfolgten nach Ansicht des EuGH damit ein „wirtschaftliches Interesse"[165].

Festhalten lässt sich hierbei zunächst, dass ein einzelner Verarbeitungsvorgang[166] vorlag und zwei unterschiedliche Zwecke. Dies ist soweit mit der Definition des Verantwortlichen vereinbar, da die Definition die **gemeinsame Entscheidung über die Zwecke** der Verarbeitung verlangt, nicht notwendigerweise die **Entscheidung über die gemeinsamen Zwecke**[167] der Verarbeitung.[168]

Irritierend wirkt bei den Ausführungen des EuGH zu den Zwecken allerdings der Verweis auf das jeweils vorhandene „wirtschaftliche Interesse" der gemeinsam Verantwortlichen. Es bleibt im Rahmen des Urteils unklar, welche Bedeutung dieses gemeinsame „wirtschaftliche Interesse" hat.[169] Das „wirtschaftliche Interesse" könnte

---

[161] So: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[162] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80. Rn. 81 hält nur das Ergebnis fest.

[163] Der EuGH verwendet dabei selbst die Formulierung „scheint [...] eingewilligt zu haben".

[164] Der EuGH spricht hier davon, dass der Plattformbetreiber für seine eigenen wirtschaftlichen Zwecke über diese personenbezogenen Daten verfügen könne. Dabei dürfte das „Verfügungsrecht" nicht entscheidend sein, sondern die bloße Erlangung der Daten, die nicht wie beim Auftragsverarbeiter nur unter Weisung des Auftraggebers erfolgen darf, vgl. Art. 28 Abs. 10 DSGVO.

[165] *Golland*, K&R 2019, 533, 535 spricht hier von der Mikro- und Makroebene der Zwecke. Vgl. zu den Begriffen a. Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 13.

[166] Der EuGH spricht hier irritierenderweise mehrfach von Erhebung und Übermittlung, also zwei Verarbeitungsvorgängen. Technisch ist dies nicht nachvollziehbar. Im Zweifel ließen sich diese beiden Vorgänge aber ohnehin als einheitliche Vorgangsreihe begreifen.

[167] So verlangen es scheinbar aber *Moos/Rothkegel*, MMR 2019, 584, 585 und *Golland*, K&R 2019, 533, 535.

[168] Letzteres wäre definitiv auch ein Fall von gemeinsam Verantwortlichen, aber eben nicht der einzige.

[169] Vgl. a. *Golland*, K&R 2019, 533, 535, der bei einem solchen Zweckverständnis mangels vernünftiger Eingrenzung durch die „Haushaltsausnahme" eine radikale Ausweitung der gemeinsamen Verantwortlichkeit prognostiziert.

im Zusammenhang mit den Ausführungen des Generalanwalts in seinen Schlussanträgen verstanden werden. Dieser hatte darauf hingewiesen, dass zwischen Websitebetreiber und Plattformbetreiber zwar keine „Zweckidentität" bestehe, allerdings auch eine „Zweckeinheit" ausreiche.[170] Es liege zwar keine identische kommerzielle Nutzung der Daten vor, allerdings würden auch kommerzielle Zwecke ausreichen, die sich wechselseitig ergänzen.[171] Dem Generalanwalt schien also eine Art Zwecksymbiose der gemeinsam Verantwortlichen vorzuschweben. Mangels expliziter Bezugnahme auf die Schlussanträge in diesem Punkt bleibt unklar, ob der EuGH die Argumentation des Generalanwalts übernommen hat.[172] Man könnte die „wirtschaftlichen Interessen" im Urteil mit den kommerziellen Zwecken in den Schlussanträgen als deckungsgleich verstehen und somit von einer Bezugnahme ausgehen. Andererseits deuten die Verwendung des Plurals „Zwecke" sowie die Einwilligung in die Verarbeitung gegenüber dem Plattformbetreiber seitens des Websitebetreibers darauf hin, dass hier nur wechselseitig hinsichtlich der Zwecke entschieden wurde. Dass eine gegenseitige Billigung des jeweils anderen Zweckes ausreichend für eine gemeinsame Entscheidung (über die Zwecke) sein könnte, wäre aber durchaus klarstellungswürdig gewesen.[173]

Zunächst stellt sich also die Frage, welche Relevanz das vom EuGH erwähnte „(wirtschaftliche) Interesse"[174] hat.[175] Ganz allgemein bedeutet Interesse nach dem Duden unter anderem Nutzen oder Vorteil.[176] Der Zweck hingegen ist das Ziel einer Handlung oder der erkennbare Sinn.[177] Der Begriff des Zweckes lässt sich also als operativ, kleinteilig und präzise begreifen, während sich der Begriff des Interesses auf einer eher undurchsichtigen und abstrakten Ebene bewegt. In diesem Zusammenhang könnte man das Interesse auch als Motivation für die Verarbeitung, den Zweck als Ziel oder Ergebnis der Verarbeitung verstehen.

[170] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 104 f.
[171] Vgl. *Jung/Hansch*, ZD 2019, 143, 147.
[172] Ablehnend: *Lee/Cross*, MMR 2019, 559, 561.
[173] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.
[174] A. in der englischen und französischen Version werden die entsprechenden Worte „economic interests" bzw. „l'intérêt économique" verwendet.
[175] *Moos/Rothkegel*, MMR 2019, 584, 585. Ebenso a. *Golland*, K&R 2019, 533, 535, der die Frage stellt, ob ein gemeinsamer Zweck konstruiert wird oder ein bislang unbekanntes Definitionselement vorliegt. Noch zu den Schlussanträgen: *Kremer*, CR 2019, 225, Rn. 13.
[176] https://www.duden.de/rechtschreibung/Interesse (abgerufen am 17.07.2024).
[177] https://www.duden.de/rechtschreibung/Zweck (abgerufen am 17.07.2024).

2. „Interesse" als gemeinsamer Zweck der gemeinsam Verantwortlichen?

Denkbar wäre, dass der EuGH das „Interesse" als Synonym zum Zweck verwenden wollte.[178] Dieses Verständnis liegt nahe, da sich die Erwähnung des „Interesses" im Zusammenhang mit den Zwecken der gemeinsam Verantwortlichen findet. Das „(wirtschaftliche) Interesse" könnte also einen gemeinsamen Zweck des Websitebetreibers und des Plattformbetreibers darstellen. So will etwa *Golland* bei dem „Interesse" eine Makroebene der Zwecke erkannt haben.[179] Diese stünde über der Mikroebene der individuellen Zwecke der gemeinsam Verantwortlichen.

Ein solches Verständnis ist aber abzulehnen. Zunächst ist die Abstraktionshöhe des „Interesses" in der konkreten Verwendung durch den EuGH problematisch. Denn im Gegensatz zur Makroebene der Vorgänge anhand der Vorgangsreihe lässt sich eine solche Makroebene für divergierende Zwecke nicht aus der DSGVO herleiten. Der Begriff der Verarbeitung ermöglicht im Rahmen der Vorgangsreihe eine Abstraktion von Zwecken gegenüber konkreten Vorgängen.[180] Verfolgen verschiedene Verantwortliche mit ihren individuellen Verarbeitungsvorgängen unterschiedliche Zwecke, die sich aber gegenseitig im Hinblick auf einen übergreifenden Zweck ergänzen,[181] besteht im Rahmen dieses übergreifenden Zweckes eine Vorgangsreihe, die die Vorgänge der verschiedenen Verantwortlichen verklammert.[182] Dabei muss dieser übergreifende Zweck aber noch hinreichend präzise sein.

In der Rechtssache Fashion ID hat der EuGH aber nur einen einzelnen Vorgang, den sich die Verantwortlichen „teilen", betrachtet,[183] nämlich die Erhebung der Besucherdaten durch den Plattformbetreiber, die wiederum von dem Websitebetreiber ermöglicht wurde. Mangels mehrerer Vorgänge lässt sich hier keine Vorgangsreihe und somit kein übergeordneter Zweck der gemeinsam Verantwortlichen bilden.

---

[178] So etwa *Schreiber*, ZD 2019, 55, 56, die im Rahmen des Zweckes a. von der Motivation spricht. Vgl. die Erwägungen zum Verbindungsgrad der Zwecke bei *Alsenoy*, CLSR[28] (2012), 25, 37 f.

[179] *Golland*, K&R 2019, 533, 535.

[180] *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 123; vgl. a. *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, [3]2022, Rn. 83; vgl. insb. für die Zweckbestimmung Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 12.

[181] Also auch nicht widersprechen.

[182] Siehe oben. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 25.

[183] Der EuGH erwähnt zwar im Urteil häufig die Erhebung und Übermittlung, technisch lässt sich ein zweiter Vorgang allerdings nicht nachvollziehen.

Die Divergenz der Zwecke in dem „Interesse“ oder dem Konzept der Zweckeinheit, so wie es der Generalanwalt verwendet,[184] folgt nicht aus individuellen Vorgängen je Verantwortlichem, sondern aus den jeweiligen Zwecken der Verantwortlichen für einen identischen Vorgang. Eine solche Abstraktion der Zwecke ist allerdings in der Definition des Verantwortlichen, auch des gemeinsam Verantwortlichen, nicht angelegt. Im Gegenteil, sie steht auch mit dem systematischen Bezug des Zweckes zur Zweckbindung[185] nach Art. 5 Abs. 1 lit. b DSGVO im Widerspruch. Demnach müssen personenbezogene Daten für festgelegte, eindeutige (und legitime) Zwecke erhoben werden. Dies hat zur Folge, dass die Zwecke der Verarbeitung hinreichend konkret und präzise bestimmt werden müssen.[186] Ein „Interesse“ oder eine Zweckeinheit hingegen, die sich auf einer derart abstrakten und darüber hinaus intransparenten Makroebene bewegt, widerspricht eklatant der präzisen Zweckbindung bzw. -festlegung gem. Art. 5 Abs. 1 lit. b sowie dem Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DSGVO.[187] Ein möglichst vager Zweck im Sinne eines „Interesses“ oder einer Zweckeinheit ermöglicht zwar gegebenenfalls die Konstruktion eines gemeinsamen Zweckes. Er ist aber nicht mehr mit dem Grundsatz der Zweckbindung vereinbar.[188] Aufgrund einer solch abstrakten Ebene dieses „Interesses“ könnte man bereits von einer fehlenden gemeinsamen Entscheidung über die Zwecke überhaupt sprechen.[189] *Golland* gibt zudem selbst zu bedenken, dass, sofern ein „gegenseitige[s] wirtschaftliche[s]

[184] In dem Fall unterschiedliche kommerzielle Zwecke bzw. kommerzielle und werbliche Zwecke: EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 105.

[185] Zu dessen Bedeutung in Form der Zweckfestlegung, insb. für das Verwaltungsrecht: *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 123 ff. Zum Begriff Zweckbindung: ebd., Rn. 127; Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 35. Zur Zweckbindung im Rahmen der DSRL: *Zezschwitz*, 3.1 Konzept der normativen Zweckbegrenzung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 11 ff.; *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 28.

[186] Statt vieler: Simitis/Hornung/Spiecker/*Roßnagel*, Art. 5 DSGVO, Rn. 72 ff. Vgl. zum Konkretisierungsgrad im Verwaltungsrecht: *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 124 ff.

[187] So wohl a. *Lee/Cross*, MMR 2019, 559, 561, die davon ausgehen, dass das „wirtschaftliche Interesse“ dem gemeinsamen Zweck entspricht. Vgl. zum Präzisionsgrad auch BT-Drs. 12/8329, S. 18 mit dem Negativbeispiel „kommerzielle Zwecke“ sowie Grabitz/Hilf[40]/*Brühann*, A 30 Art. 6 DSRL, Rn. 9 mit dem Negativbeispiel „geschäftsmäßige Verarbeitung“.

[188] Vgl. *Specht-Riemenschneider/Schneider*, GRUR Int 2020, 159, 162.

[189] *Kremer*, CR 2019, 225, Rn. 13.

Profitieren" als gemeinsamer Zweck ausreiche, hiervon viele verschiedene Varianten des Zusammenwirkens betroffen wären.[190]

Nirgendwo in der DSGVO ist schließlich ersichtlich, dass der Begriff der Zwecke in Art. 4 Nr. 7 DSGVO anders oder weiter zu verstehen ist als die Zweckbindung in Art. 5 Abs. 1 lit. b DSGVO. Will man die notwendige Präzision der Zweckfestlegung in Art. 5 Abs. 1 lit. b DSGVO also umgehen, gelingt dies nur, wenn man keinen systematischen Bezug zwischen den beiden Normen herstellt. Dann wäre die Wortwahl in Art. 4 Nr. 7 DSGVO mit „Zwecke" allerdings gesetzgeberisch sehr unglücklich.

3. „Interesse" als berechtigtes Interesse der gemeinsam Verantwortlichen?

Ungeachtet des Kontextes der Erwähnung des „Interesses", also im Rahmen der Ausführungen zum Zweck, könnte man es ebenso wie den Zweck nach der Systematik der DSRL[191] verstehen. So taucht das Wort Interesse in der DSRL prominent im Rahmen der Verarbeitungsrechtfertigungstatbestände in Art. 7 DSRL auf, insbesondere in lit. f[192] als berechtigtes Interesse. In der Rechtssache Fashion ID, wenn auch in Antwort auf Vorlagefrage 4,[193] nicht 2[194], stellt der EuGH zudem fest, dass jeder der gemeinsam Verantwortlichen ein berechtigtes Interesse oder allgemeiner einen Verarbeitungsrechtfertigungstatbestand benötige.[195] Die englische und französische Sprachfassung der Entscheidung verwenden zudem Begriffe, die, ebenso wie die deutsche Fassung, sprachlich eine Bezugnahme auf Art. 7 lit. f DSRL nahelegen. Die Verwendung des Begriffs des „Interesses" erscheint also nicht als eine zufällige stilistische Wahl.

Versteht man allerdings die Verwendung des Begriffs „Interesse" als systematischen Verweis auf das berechtigte Interesse, ist damit kein Erkenntnisgewinn verbunden. So sagt der Verarbeitungsrechtfertigungstatbestand nichts über die konkreten Zwecke der Verarbeitung aus,[196] sondern sorgt nur für die Rechtmäßigkeit der Verarbeitung bzw. des Zweckes der Verarbeitung gem. Art. 6 Abs. 1 lit. b DSRL.[197]

---

[190] *Golland*, K&R 2019, 533, 535.
[191] Die Rechtssache Fashion ID betraf noch die DSRL.
[192] In der DSGVO Art. 6 Abs. 1 lit. f.
[193] Diese beschäftigt sich damit, auf wessen „berechtigtes Interesse" abzustellen ist.
[194] Diese beschäftigt sich damit, wer für die Erhebung der Daten verantwortlich ist.
[195] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 96 f.
[196] Maximal im Sinne einer Kategorie nach Art. 6 Abs. 1 DSGVO.
[197] Vgl. a. *Moos/Rothkegel*, MMR 2019, 584, 585.

4. „Interesse" als neues Definitionselement der gemeinsam Verantwortlichen?

Begreift man das „Interesse" weder als Zweck noch als berechtigtes Interesse, könnte es sich noch um ein neues, ungeschriebenes Definitionselement handeln. Sollte eine solche Rechtsfortbildung die Intention des EuGH gewesen sein, wäre dies aber, allein aufgrund der erwähnten systematischen Erwägungen, erheblich begründungsbedürftiger.

Golland stellt nichtsdestotrotz die Hypothese auf, der EuGH habe mit dem Interesse ein weiteres Definitionselement der gemeinsam Verantwortlichen begründet.[198] Eine gemeinsame Verantwortlichkeit bestünde demnach nur unter der zusätzlichen Voraussetzung des „gegenseitige[n] wirtschaftliche[n] Profitieren[s]". Sofern Akteure diese Voraussetzung nicht erfüllen würden, wären sie keine gemeinsam Verantwortlichen und müssten die weitergehenden Pflichten und Haftung nicht beachten.[199] Nicht-kommerzielle Akteure wären umgekehrt also insoweit privilegiert.[200] Hierbei räumt *Golland* allerdings ein, dass diese weitere Voraussetzung im Widerspruch zum Urteil in der Rechtssache Jehovan todistajat[201] stünde. In dieser Entscheidung hatte der EuGH die gemeinsame Verantwortlichkeit einer Glaubensgemeinschaft und deren Mitglieder im Rahmen des Zweckes der Verkündigungstätigkeit angenommen. Dort handelte es sich um nicht-kommerzielle Akteure, die darüber hinaus auch denselben Zweck verfolgten.[202]

Neben dem Widerspruch zur vorherigen Rechtsprechung stünde diese zusätzliche Voraussetzung auch systematisch wie gesetzgebungstechnisch mit den Ausnahmen vom Anwendungsbereich in Art. 2 Abs. 2 DSGVO, insbesondere der Haushaltsausnahme, im Widerspruch. In Art. 2 Abs. 2 DSGVO wird anhand eng auszulegender Ausnahmetatbestände ein bestimmter Verarbeitungskontext privilegiert,[203] indem dieser nicht der DSGVO unterfällt. Bei der zusätzlichen Voraussetzung des „gegenseitige[n] wirtschaftliche[n] Profitieren[s]" würden Akteure, die diese Voraussetzung erfüllen, hingegen mit den Pflichten und der Haftung einer gemeinsamen Verantwortlichkeit belastet. Unklar wäre zudem, wann die Grenze eines

[198] Ähnlich *Lee/Cross*, MMR 2019, 559, 562 mit dem „quasivertraglichen Bezug", die aber Übertragbarkeitsprobleme bei der Rechtsprechung aus Fashion ID sehen.

[199] Vgl. zu einem Kommerzialitätskriterium auch *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 76 ff.

[200] *Golland*, K&R 2019, 533, 535; *Golland*, ZD 2020, 397, 399.

[201] Dazu: Kapitel 4 B. II. Jehovan todistajat.

[202] Daher ist der Sachverhalt bereits nicht vergleichbar. Zum gemeinsamen Zweck: Kapitel 4 E. Die Zwecke der Verarbeitung als Entscheidungsobjekt.

[203] Überaus deutlich: EuGH, Urteil vom 09.07.2020 – C-272/19 (VQ/Hessen) = NVwZ 2020, 1497, Rn. 66 ff.; EuGH, Urteil vom 04.05.2017 – C-13/16 (Rigas) = DAR 2017, 698, Rn. 30.

„gegenseitige[n] wirtschaftliche[n] Profitieren[s]“ oder „wirtschaftlichen Interesses“ unterschritten würde. Es ist nicht nachvollziehbar, warum der Unionsgesetzgeber nicht entweder eine Ausnahme von den Pflichten und Haftung für nicht-kommerzielle Akteure in Art. 26 DSGVO selbst normiert hätte oder jedenfalls bei den Voraussetzungen der gemeinsamen Verantwortlichkeit positiv das „gegenseitige[n] wirtschaftliche[n] Profitieren[s]“ oder „wirtschaftliche Interesse“ geregelt hätte. Anstatt einen engen Bereich zu privilegieren – was die übliche Regelungstechnik in der DSGVO darstellt –, würde durch diese zusätzliche Voraussetzung per Richterrecht ein weiter, unklar konturierter Verarbeitungskontext benachteiligt.

Denkbar wäre noch, dass sich der EuGH mit dem „(wirtschaftlichen) Interesse“ an seine Rechtsprechung im Immaterialgüterrecht[204] anlehnt. Dann würde das „wirtschaftliche Interesse“, vergleichbar mit der Gewinnerzielungsabsicht, eine bestimmte Sorgfaltspflicht in Verarbeitungsszenarien mit mehreren Akteuren begründen, die bei Verantwortlichen mit nicht-wirtschaftlichen Interessen nicht erforderlich wäre. Akteure mit „wirtschaftlichem Interesse“ müssten also gegebenenfalls höhere Sorgfaltsmaßstäbe bei der Auswahl von gemeinsam Verantwortlichen und der Überwachung der Verarbeitungen befolgen. Problematisch an dieser vermeintlichen Bezugnahme ist dreierlei.[205] Zunächst kennt die Auftragsverarbeitung in Art. 28 DSGVO als Verarbeitungsszenario mit mehreren Akteuren keine Differenzierung anhand eines (nicht-)wirtschaftlichen Interesses des Verantwortlichen. Zum anderen kennt das Datenschutzrecht bislang auch keine gesetzliche oder richterliche Fixierung von Absichts- oder Kenntniselementen im Hinblick auf die Entscheidung.[206] Wenigstens ein Verweis auf die genannte Rechtsprechung wäre daher notwendig gewesen, um eine solche Verbindung herzustellen. Zuletzt würde auch dieses Verständnis eines neuen Definitionselements mit der Regelungstechnik der engen Ausnahmen vom Anwendungsbereich im Konflikt stehen.[207]

[204] EuGH, Urteil vom 08.09.2016 – C-160/15 (GS Media/Sanoma ua) = GRUR 2016, 1152, Rn. 47, 51.

[205] Wenn man bereit ist zu übersehen, dass wirtschaftliches Interesse und Gewinnerzielungsabsicht schon vom Wortlaut her nicht übereinstimmen.

[206] Dazu: Kapitel 2 E. I. Vorfrage: Notwendige Kenntniselemente der Entscheidung. Vgl. hierzu a. die Erwägungen in EuGH, Urteil vom 08.09.2016 – C-160/15 (GS Media/Sanoma ua) = GRUR 2016, 1152, dazu: *Ohly*, GRUR 2016, 1155, Rn. 9.

[207] Vgl. EuGH, Urteil vom 04.05.2017 – C-13/16 (Rigas) = DAR 2017, 698, Rn. 30.

5. „Interesse" als Abgrenzung zum Auftragsverarbeiter?

Man kann die Ausführungen des EuGH zu den Zwecken und dem „Interesse" allerdings auch noch anders verstehen. Auffallend ist im Vergleich zwischen den Schlussanträgen und dem Urteil in der Rechtssache Fashion ID, dass der Generalanwalt mit der Zweckeinheit ein gemeinsames Element der gemeinsam Verantwortlichen betont. Der EuGH hält im Urteil hingegen fest, dass ein wirtschaftliches Interesse sowohl auf Seiten des Websitebetreibers wie auch des Plattformbetreibers vorliegt. Folglich muss sich aus dem beidseitigen „(wirtschaftlichen) Interesse" nicht zwangsläufig ein verbindendes Element ergeben. Vielmehr könnte dadurch auch nur eine Art Gleichrangigkeit der Akteure attestiert werden. Diese Feststellung der Gleichrangigkeit würde insofern Sinn ergeben, dass eine Abgrenzung zur Auftragsverarbeitung erfolgt.[208] Mit einem eigenen wirtschaftlichen Interesse wäre eine Auftragsverarbeitung ausgeschlossen, da sich der gemeinsame Verantwortliche dann nach Art. 28 Abs. 10 DSGVO nicht nur der Zweckbestimmung der anderen gemeinsam Verantwortlichen im Sinne einer Auftragsverarbeitung unterwirft.

Auch dieses Verständnis des „Interesses" ist allerdings nicht unproblematisch. So verfolgt der Auftragsverarbeiter regelmäßig ein wirtschaftliches Interesse, nämlich der vertraglichen Gegenleistung. Denkbar sind zudem vertragliche Szenarien, in denen Teil der Entlohnung die Möglichkeit der eigenen wirtschaftlichen Verwendung der Daten ist.[209] Abgrenzen lässt sich das wirtschaftliche Interesse an der Entlohnung aber insofern, dass es Folge der Verarbeitung ist, der Auftragsverarbeiter aber nicht an der Verarbeitung per se ein eigenes Interesse hat.[210] Abseits dessen ist die Abgrenzung des Verantwortlichen zum Auftragsverarbeiter insgesamt sinnvoller im Rahmen des Eigeninteresses als Aspekt der Entscheidung über die Verarbeitung zu verorten.[211]

Solange der Auftraggeber hinsichtlich der nachgelagerten Verarbeitung des Auftragnehmers keine Entscheidungsmacht hätte, bestünde auch keine gemeinsame Verantwortlichkeit zwischen dem vermeintlichen Auftraggeber und

[208] Vgl. BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 28 f.

[209] Vgl. dazu *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18 Beispiel 3 und ebd., 23 Beispiel 6. Die Art. 29-Datenschutzgruppe geht in beiden Beispielen von einer eindeutigen Stellung als Verantwortlicher aus. Unklar ist allerdings, ob eine Billigung der Nutzung durch den Auftragsverarbeiter seitens des ursprünglich Verantwortlichen Konsequenzen hätte. Die einseitige Zweckbestimmung (also ohne Abstimmung mit dem anderen Verantwortlichen) würde bereits nach Art. 28 Abs. 10 DSGVO eine Stellung als Verantwortlicher bedeuten.

[210] So a.: *Hanloser*, ZD 2019, 455, 459.

[211] Dazu vertiefend: Kapitel 2 G. IV. Das Eigeninteresse als eigener Zweck?

Auftragnehmer.[212] Dabei wäre die eigene Verwendung dieser Daten durch den Auftragsverarbeiter, als eine der Auftragsverarbeitung nachgelagerte Verarbeitung, natürlich keine Auftragsverarbeitung mehr. Hat der Auftraggeber hingegen Entscheidungsmacht im Hinblick auf die nachgelagerte Verarbeitung könnte bereits für die ursprüngliche Auftragsverarbeitung eigentlich eine gemeinsame Verantwortlichkeit vorliegen. Die Zurverfügungstellung der Daten durch den Auftraggeber als Entlohnung müsste entweder als zweite Übermittlung nach der Durchführung der Auftragsverarbeitung konstruiert werden oder alternativ die Übermittlung zur Durchführung der Auftragsverarbeitung auch (additiv) den Zweck der Entlohnung durch die Daten beinhalten. Letzteres dürfte aber im Konflikt mit der Pflicht zur Rückgabe bzw. Löschung der Daten nach Art. 28 Abs. 3 lit. g DSGVO stehen.

6. „Interesse" als Zweckkomplementarität

Das vom EuGH erwähnte „Interesse" in der Rechtssache Fashion ID lässt sich schließlich auch so verstehen, dass der Zweck eines gemeinsam Verantwortlichen nicht dem erkennbaren oder vermuteten Willen eines anderen gemeinsam Verantwortlichen widerspricht. Folglich wäre dann „Interesse" als „im Interesse" oder „mit hypothetischer Billigung des [anderen gemeinsam Verantwortlichen]" zu verstehen.[213] Diese gegenseitige Billigungsfähigkeit der Zwecke kann man, in Abgrenzung zur Zweckkompatibilität in Art. 6 Abs. 4 DSGVO, als Zweckkomplementarität[214] bezeichnen.[215] Die jeweiligen eigenen Zwecke der gemeinsam Verantwortlichen ergänzen sich gegenseitig im Rahmen einer Billigungsfähigkeit. Sofern bei divergierenden Zwecken der gemeinsam Verantwortlichen im Rahmen der gemeinsamen Entscheidung eine Billigung der fremden Zwecke zu prüfen ist, ist die Zweckkomplementarität abseits einer expliziten Billigung objektive Voraussetzung für eine implizite Billigung.[216] Abseits eines erkennbaren Willens zur Billigung der Zwecke

[212] Auftraggeber (Verantwortlicher) A beauftragt Auftragnehmer (Auftragsverarbeiter) B mit Verarbeitung Y. Nach Abschluss der Verarbeitung Y darf Auftragnehmer B als Teil der Entlohnung von A frei über die Verwendung der Daten verfügen (die Rechtmäßigkeit der Verarbeitung unterstellt). Auftragnehmer B führt mit den Daten aus Y die Verarbeitung Z durch. An Verarbeitung Z hat A keine Entscheidungsmacht. Folglich ist nur B für Verarbeitung Z Verantwortlicher.

[213] Unberechtigt daher die Kritik bei: Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 46.

[214] Alternativ bietet sich auch der Begriff Zweckförderlichkeit an. Allerdings unterstreicht Zweckkomplementarität besser den Austauschcharakter.

[215] Vgl. die „converging decisions" bei *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

[216] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

der anderen gemeinsam Verantwortlichen ist also zu prüfen, ob ein objektiver Dritter aus Perspektive eines gemeinsam Verantwortlichen die Zwecke der anderen billigen würde. Denkbar wäre dies etwa dann, wenn die Zwecke der anderen gemeinsam Verantwortlichen in seinem „wirtschaftlichen Interesse" liegen würden. Die Prüfung der Zweckkomplementarität ist bei einem gemeinsamen Zweck hingegen hinfällig. Denn dann besteht nicht die Notwendigkeit der Billigung fremder Zwecke.

Dieses Verständnis des „Interesses" lässt sich mit der Rechtsprechung des EuGH aus den Rechtssachen Wirtschaftsakademie und Fashion ID vereinbaren. Denn der Plattformbetreiber hat ein Interesse an der Nutzung seiner Angebote, also an der Eröffnung einer Fanpage (Seite auf der Plattforminfrastruktur) bzw. dem Einbau seines Social Plugins in eine Website, um an die Daten der Besucher der Fanpage bzw. Website zu gelangen. Welche konkreten Zwecke der Fanpage- bzw. Websitebetreiber mit der Nutzung dieser Angebote verfolgt, dürfte für den Plattformbetreiber grundsätzlich unerheblich sein, solange er nicht von deren Zwecken Abstand genommen hat.[217] Der Plattformbetreiber hat für seine eigenen Zwecke, die Erhebung der Besucherdaten, also grundsätzlich ein Interesse daran, dass der Fanpage- bzw. Websitebetreiber wiederum dessen eigene Zwecke verfolgt. Der Fanpage- bzw. Websitebetreiber hat für seine eigenen Zwecke andererseits ein Interesse daran, dass der Plattformbetreiber die Daten der Besucher, als Voraussetzung der Nutzung der Angebote des Plattformbetreibers, erhält. Im Rahmen der faktischen Nutzung des Angebots erfolgt dann eine implizite Billigung der Zwecke des Plattformbetreibers durch den Fanpage- oder Websitebetreiber. In der Bereitstellung des Angebots erfolgt im Rahmen der vertraglichen und technischen Bedingungen eine implizite Billigung der Zwecke des Fanpage- oder Websitebetreibers durch den Plattformbetreiber.[218]

Der EuGH erwähnt im Rahmen seiner Analyse der Mittel der Verarbeitung in der Rechtssache Fashion ID, dass diese „zum Zweck" der Erhebung und Übermittlung der personenbezogenen Daten der Websitebesucher eingesetzt werden.[219] Für den Websitebetreiber macht dieser (vermeintliche)[220] Zweck nur Sinn, wenn er Teil eines Austauschverhältnisses ist. Deutlich wird dies auch an der Wortwahl des EuGH in Rn. 80: die Verarbeitungsvorgänge liegen im beiderseitigen wirtschaftlichen Interesse,

[217] Etwa durch Nutzungsbedingungen, technische Maßnahmen oder ähnliches.

[218] Zur Billigung: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung. Eine explizite Billigung kann nicht erfolgen, da die Nutzung der Bereitstellung nachgelagert ist und üblicherweise kein direkter Kontakt zwischen beiden besteht.

[219] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77.

[220] Dabei ist bereits fraglich, ob das „zum Zweck" der deutschen Fassung sich auf die Zwecke der Verarbeitung bezieht oder eine rein stilistische Wahl ist. Die spanische Sprachfassung des Urteils verwendet in Rn. 77 und 80 jedenfalls unterschiedliche Begriffe.

da der Plattformbetreiber damit eigene wirtschaftliche Zwecke verfolgen kann, während der Websitebetreiber den Zweck der Optimierung der Werbung für seine Produkte verfolgt. Damit wird deutlich, dass das „Interesse" nicht Synonym für den Zweck ist.

Insgesamt sind die Ausführungen des EuGH zum „(wirtschaftlichen) Interesse" in der Rechtssache Fashion ID also so zu verstehen, dass, wenn gemeinsam Verantwortliche jeweils eigene Zwecke verfolgen, die jeweiligen Zwecke im Interesse der anderen gemeinsam Verantwortlichen liegen müssen.[221] Folglich wäre das „Interesse" nicht bedeutungsgleich mit dem Zweck, diesem jedoch inhaltlich angenähert.[222] Letztlich läuft es mit der Zweckkomplementarität begrifflich auf die bereits vom Generalanwalt erwähnte Zweckeinheit hinaus.[223] Anders als bei den Schlussanträgen des Generalanwalts begründet sich aus der Zweckkomplementarität allerdings kein gemeinsamer Zweck, sondern nur eine Vereinbarkeit der unterschiedlichen Zwecke der gemeinsam Verantwortlichen. Die Zweckkomplementarität ersetzt zudem nicht ein gemeinsames Element der Verantwortlichen.[224] Sie deutet nur an, dass eine gemeinsame Entscheidung über die Zwecke möglich ist und impliziert diese, abseits einer expliziten Entscheidung im Sinne einer Billigung.[225]

Abzugrenzen ist das „(wirtschaftliche) Interesse" schließlich vom „Eigeninteresse"[226] in dem Urteil in der Rechtssache Fashion ID. In Rn. 68 des Urteils führt der EuGH aus, dass eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als Verantwortlicher angesehen werden kann. Das „Eigeninteresse" aus Rn. 68 lässt sich als Entscheidungsautonomie über die Zwecke und wesentlichen[227] Elemente der Mittel verstehen,[228] während das „(wirtschaftliche)[229] Interesse" in Rn. 80 die Vereinbarkeit der jeweiligen Zwecke gemeinsam Verantwortlicher bestimmt.

---

[221] Vgl. *Kremer*, CR 2019, 225, Rn. 14. Ähnlich wohl a.: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 42. Irritierend wirkt dabei aber der gemeinsame Austauschzweck.

[222] Anders *Hanloser*, ZD 2019, 455, 459, der in den Ausführungen zum Interesse eine Aufweichung des Begriffs des Zweckes erkennen möchte.

[223] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 105.

[224] Dazu: Kapitel 4 H. II. Gemeinsame Zwecke oder Mittel als Identitätsgarant der Verarbeitung.

[225] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

[226] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 68.

[227] Dazu: Kapitel 2 D. Mittel.

[228] Zum Eigeninteresse: Kapitel 2 G. IV. Das Eigeninteresse als eigener Zweck?

[229] Hierbei soll das „wirtschaftlich" nur verdeutlichen, dass es sich nicht um das Eigeninteresse in

II. Die „Einwilligung" in eine Verarbeitung als Einigung auf einen gemeinsamen Zweck?

Die Verfechter der Notwendigkeit eines gemeinsamen Zweckes als Voraussetzung für die gemeinsame Verantwortlichkeit scheinen die „Einwilligung"[230] in einen fremden Zweck – in der Rechtssache Fashion ID die Einwilligung in die Erhebung der personenbezogenen Daten seitens Facebook durch die Verwendung des Social Plugins – als Einigung auf einen gemeinsamen Zweck zu konstruieren. Somit würde in der Rechtssache Fashion ID das „wirtschaftliche Interesse" zum gemeinsamen Zweck erhoben. Damit erreicht das „wirtschaftliche Interesse" als vermeintlicher Zweck allerdings einen Abstraktionsgrad, der kaum noch mit dem Konzept der Zweckfestlegung und -bindung aus Art. 5 Abs. 1 lit. b DSGVO vereinbar ist. Aufgrund des Charakters eines Austauschverhältnisses bezeichnen *Lee/Cross* die „Einwilligungen" in die gegenseitigen Zwecke als „quasivertraglichen Bezug"[231] der Zwecke.

Neben dem fehlenden Anklingen der Notwendigkeit eines gemeinsamen Zweckes in der Definition des Verantwortlichen spricht allerdings auch die Rechtsprechung des EuGH gegen eine solche Notwendigkeit. In der maßgeblichen Rn. 80 in dem Urteil zu der Rechtssache Fashion ID ist nämlich keinesfalls die Rede von einem gemeinsamen Zweck.[232] Das Wort „gemeinsam" taucht dort nicht einmal auf. Versteht man die Optimierung der Werbung für die eigenen Produkte als den Zweck des Websitebetreibers und die Verwendungsmöglichkeit der erlangten Daten für eigene Zwecke als Zweck des Plattformbetreibers, besteht kein gemeinsamer Nenner der Zwecke. Deutlich wird das Fehlen eines gemeinsamen Zweckes auch anhand der Formulierung „[...] über diese Daten für ihre eigenen wirtschaftlichen Zwecke verfügen zu können [...]" in Bezug auf den Plattformbetreiber. Der Websitebetreiber auf der anderen Seite willigt als Bedingung für wiederum seine eigenen Zwecke in die Verarbeitung der personenbezogenen Daten ein.[233] Inwiefern hierbei von einer Einigung auf einen gemeinsamen Zweck gesprochen werden kann, ist nicht nachvollziehbar. Dies wird noch deutlicher dadurch, dass sich die Einwilligung des

EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 68, sondern um das Interesse in Rn. 80 handelt.

[230] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80.

[231] Kritisch: *Lee/Cross*, MMR 2019, 559, 561 f. Vgl. zum Begriff a. BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 42. *Hanloser*, ZD 2019, 455, 459 spricht von einer wechselseitigen Förderungswirkung.

[232] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80.

[233] *Kollmar*, NVwZ 2019, 1740, 1741 versteht die missverständliche Verwendung des Begriffs Einwilligung als Abgrenzung zu einer Störerhaftung.

Websitebetreibers rein grammatikalisch auf die Verarbeitung und nicht einmal auf den Zweck des Plattformbetreibers bezieht.[234] Festhalten lässt sich anhand der Ausführungen des EuGH nur, dass der Websitebetreiber und Plattformbetreiber jeweils vergleichbare wirtschaftliche Interessen verfolgen, die sich gegenseitig bedingen.[235] Eben dies wird durch das bereits dargestellte Konzept der Zweckkomplementarität abgedeckt.

Setzt man trotz der genannten Argumente dennoch einen gemeinsamen Zweck für eine gemeinsame Verantwortlichkeit voraus, würde dies deren Anwendungsbereich stark einschränken. So ist es leichter eine Billigung von Zwecken anhand von Zweckkomplementarität anzunehmen als die Einigung auf einen gemeinsamen Zweck oder das Zu-Eigen-Machen eines fremden Zweckes zu begründen.[236] Auch bei einer Zweckkomplementarität bestände immer noch die Möglichkeit ungewünschte Zwecke durch entsprechende Abwehrmaßnahmen wie AGBs oder technische Maßnahmen zu missbilligen.[237] Das Erfordernis eines gemeinsamen Zweckes würde vor allem antizipierte Verarbeitungen, die sich an noch unbekannte Akteure richten, wie etwa in der Rechtssache Fashion ID, ausschließen. Denn eine Einigung auf einen gemeinsamen Zweck könnte abseits eines Zu-Eigen-Machens nicht erfolgen. Eine solche Einigung würde ein direktes Verhandeln mit dem anderen potenziell gemeinsam Verantwortlichen voraussetzen. Dies wäre gerade bei massenhaft angebotenen Verarbeitungen nicht möglich. Eine solche Einschränkung steht auch erkennbar im Widerspruch zur Absicht der Art. 29-Datenschutzgruppe verschiedenste Formen der Kollaboration zu erfassen.[238]

III. Position der Aufsichtsbehörden

1. Europäischer Datenschutzbeauftragter (EDPS)

Die Position des EDPS zur vermeintlichen Notwendigkeit eines gemeinsamen Zweckes ist nicht eindeutig. Dies wiederum dürfte den Urteilen des EuGH geschuldet sein, die selbst keine klare Systematik erkennen lassen. Insgesamt fordert der EDPS ein „same

[234] „[...] stillschweigend in das Erheben [...] und deren [...] Übermittlung eingewilligt zu haben."
[235] *Kollmar*, NVwZ 2019, 1740, 1741.
[236] Vgl. *Moos/Rothkegel*, MMR 2019, 584, 585 f.
[237] Ein Vergleich mit den Nutzungsvorgaben von Creative-Commons-Lizenzen (wie etwa keine kommerzielle Nutzung oder keine Veränderung des Werkes) bietet sich an.
[238] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23.

general objective (or purpose)“[239], ein „ ‘general’ level of complementarity and unity of purpose“[240] oder „converge on the same general objective (or purpose)“[241]. Dabei scheint das Vorliegen eines „same general objective (or purpose)“ allerdings alternativ zu den „jointly determined means“[242] möglich zu sein. Ein „identischer allgemeiner Zweck“ oder eine „Zweckeinheit“ scheint also auch bei nicht gemeinsam festgelegten Mitteln ausreichend. Unklar bleibt allerdings, ob der EDPS das „ ‘general’ level of complementarity of purpose and unity of purpose“ als gemeinsamen Zweck erachtet oder ob die Komplementarität der Zwecke als zusätzliche Voraussetzung, im Sinne einer Einschränkung, neben die Voraussetzung der gemeinsamen Mittel tritt. Je nach Verständnis wäre die Zweckkomplementarität dann entweder alternativ oder kumulativ zu den gemeinsamen Mitteln notwendig.[243] Das Verständnis der kumulativen Voraussetzung entspricht der hier vorgeschlagenen implizierten Billigung aufgrund von Zweckkomplementarität.[244]

2. Europäischer Datenschutzausschuss (EDPB)

Der EDPB differenziert bei der gemeinsamen Entscheidung über Zwecke zwischen einem identischen Zweck und gemeinsamen Zwecken.[245] In beiden Fällen soll eine gemeinsame Verantwortlichkeit bestehen. So scheinen gemeinsame Zwecke dann vorzuliegen, wenn Akteure Zwecke verfolgen, die eng verbunden oder komplementär sind.[246] Dies kann etwa dann der Fall sein, wenn ein wechselseitiger Vorteil aus der Verarbeitung erwächst.[247] Dieser Vorteil sei aber nur ein Indikator und nicht entscheidend. Die Urteile in den Rechtssachen Wirtschaftsakademie und Fashion ID

[239] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 10.

[240] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 23.

[241] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 24.

[242] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 24.

[243] Vgl. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 10, 24.

[244] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

[245] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 59.

[246] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 60.

[247] Unklar hinsichtlich der Frage, ob ein identischer oder gemeinsamer Zweck vorliegt: *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 43.

sollen jeweils für einen gemeinsamen Zweck stehen.[248] Voraussetzung für eine gemeinsame Verantwortlichkeit sei zudem, dass alle gemeinsam Verantwortlichen sich an der Entscheidung über die Zwecke und Mittel der Verarbeitung beteiligen. Dies sei etwa möglich im Rahmen von „converging decisions".[249] Diese konvergenten Entscheidungen sollen dann vorliegen, wenn Entscheidungen sich gegenseitig ergänzen und für die Durchführung der Verarbeitung in der Weise notwendig sind, dass sie eine spürbare Auswirkung auf die Entscheidung über die Zwecke und Mittel der Verarbeitung haben.[250] Ein wichtiges Kriterium, um das Vorliegen konvergenter Entscheidungen festzustellen sei, ob die Verarbeitung nur durch die Beteiligung beider Akteure an den Zwecken und Mitteln der Verarbeitung möglich sei, die Verarbeitung beider Akteure also untrennbar miteinander verbunden sei.

Das vom EDPB vorgeschlagene Verständnis von gemeinsamen Zwecken scheint sinnvoller und trennschärfer im Rahmen der Billigung von Zwecken, etwa implizit durch Zweckkomplementarität, anwendbar.[251] Die Zweckkomplementarität als Konzept lässt sich anhand des Bezugspunkts der „converging decisions" – also der Zwecke und Mittel der Verarbeitung – erahnen.[252] So seien bei allen kommerziellen Vereinbarungen notwendigerweise „converging decisions" vorhanden.[253] Die „converging decisions" könnten sich aber nur auf die Zwecke und Mittel der Verarbeitung beziehen.

IV. Fazit

Festhalten lässt sich insgesamt, dass ein gemeinsamer Zweck bei gemeinsam Verantwortlichen nicht zwingend erforderlich ist. Vielmehr können gemeinsam Verantwortlichen eigene, sich ergänzende, oder auch gemeinsame Zwecke verfolgen.[254] Ob sich Zwecke ergänzen, kann im Rahmen des Kriteriums der Zweckkomplementarität beurteilt werden.

---

[248] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 60 f.

[249] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

[250] Vgl. *Gierschmann*, ZD 2020, 69, 71. Ablehnend: *Lee/Cross*, MMR 2019, 559, 561.

[251] Dazu: Kapitel 4 E. I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen.

[252] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

[253] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55 Fn. 20.

[254] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 33; *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 505.

F. Die Mittel der Verarbeitung als Entscheidungsobjekt

Neben der bereits erörterten Frage, ob ein gemeinsamer Zweck für eine gemeinsame Verantwortlichkeit erforderlich ist, stellt sich dieselbe Frage auch hinsichtlich gemeinsamer Mittel. Denn sofern man das Definitionselement „gemeinsam" auf die Zwecke beziehen kann, liegt es ebenso nahe, es auch auf die Mittel zu beziehen. Die Notwendigkeit gemeinsamer Mittel wird in der Literatur aber im Gegensatz zu den gemeinsamen Zwecken kaum beleuchtet. Dies ist insoweit verwunderlich, als dass die verwendeten Mittel auch die personenbezogenen Daten selbst betreffen, jedenfalls nach dem Verständnis der Art. 29-Datenschutzgruppe.[255] Anhand der verarbeiteten personenbezogenen Daten lässt sich überhaupt erst die Identität eines Verarbeitungsvorgangs zwischen verschiedenen Verantwortlichen herstellen. Dieser Verarbeitungsvorgang ist wiederum gerade Bezugspunkt für eine potenzielle gemeinsame Verantwortlichkeit.[256] Genauso wie bei der Frage der Notwendigkeit eines gemeinsamen Zweckes,[257] lässt sich auch die Notwendigkeit gemeinsamer Mittel nicht dem Wortlaut der Definition der gemeinsam Verantwortlichen entnehmen. Die Definition spricht nur von einer gemeinsamen Entscheidung bzw. Festlegung der Zwecke und Mittel der Verarbeitung.

I. Inhalt der Mittel?

Im Gegensatz zum gemeinsamen Zweck stellt sich bei den gemeinsamen Mitteln aber das Problem, dass bereits nicht restlos klar ist, was genau das Definitionselement Mittel beinhaltet. So findet sich in der Rechtsprechung des EuGH[258] keine Bezugnahme auf die Differenzierung der Art. 29-Datenschutzgruppe bzw. des EDPB zwischen wesentlichen und unwesentlichen Elementen der Mittel.[259] Eine solche Differenzierung sollte dennoch vorgenommen werden. Für die gemeinsame Entscheidung über die Mittel sind gerade die wesentlichen Elemente der Mittel sehr wichtig. Diese sollten, wie bereits dargestellt, vor allem Art. 28 Abs. 3 S. 1 DSGVO entnommen werden. Primär die Art der zu verarbeitenden personenbezogenen Daten sowie die Kategorie betroffener Personen beschreiben überhaupt erst den Zuschnitt oder die Identität der Verarbeitung.

---

[255] Dazu: Kapitel 2 D. Mittel; *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 33 versteht die Parametrierung in Wirtschaftsakademie hingegen zumindest a. als Entscheidung über die Zwecke.

[256] Vgl. EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 76. In diese Richtung ist wohl *Kremer*, CR 2019, 225, Rn. 12 zu verstehen.

[257] Dazu: Kapitel 4 E. Die Zwecke der Verarbeitung als Entscheidungsobjekt.

[258] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[259] Dazu: Kapitel 2 D. Mittel.

Werden zwischen verschiedenen Akteuren andere Arten von Daten oder von anderen betroffenen Personen verarbeitet, ist es äußerst zweifelhaft, ob überhaupt eine identische Verarbeitung zwischen diesen Akteuren vorliegt. Ohne den gemeinsamen Bezugspunkt für die gemeinsame Verantwortlichkeit ist eine solche aber gar nicht erst denkbar. Daneben ist aber auch die Dauer der Verarbeitung wichtig, da sie durch die Möglichkeit von deren Beendigung Rückschlüsse auf den Einfluss der sie bestimmenden Partei bietet. Schließlich steht die Auswahl der verarbeiteten Daten im engen Zusammenhang mit dem sachlichen Anwendungsbereich der DSGVO gem. Art. 2 Abs. 1 sowie den besonderen Kategorien personenbezogener Daten gem. Art. 9 DSGVO. Auch die anderen wesentlichen Elemente der Mittel weisen aber einen Bezug zu zentralen Normen der DSGVO wie etwa den Grundsätzen der Verarbeitung gem. Art. 5 Abs. 1 oder der Verarbeitung unter der Aufsicht gem. Art. 29 auf. Eine ähnliche Relevanz kann bei den unwesentlichen Elementen der Mittel hingegen grundsätzlich nicht angenommen werden. Daher wäre es auch übertrieben bezüglich der unwesentlichen Elemente der Mittel eine Identität zwischen verschiedenen gemeinsam Verantwortlichen zu fordern.[260] Daher beschränkt sich die nachfolgende Analyse der Notwendigkeit gemeinsamer Mittel auf die wesentlichen Elemente der Mittel.

II. Zugriff auf Daten oder Infrastruktur der Verarbeitung durch alle gemeinsam Verantwortlichen?

Denkbar ist zunächst, dass gemeinsame Mittel ein Zugriffsrecht auf oder Sachherrschaft über diese Mittel implizieren. Der EuGH hat allerdings wiederholt festgestellt, dass ein Zugang zu den verarbeiteten Daten nicht seitens aller gemeinsam Verantwortlichen erforderlich ist.[261] Daher ist erst recht die Verfügungsgewalt oder die Sachherrschaft über die übrigen gemeinsamen Mittel für alle gemeinsam Verantwortlichen entbehrlich.[262] Dasselbe gilt auch für die Funktionsherrschaft aller gemeinsam Verantwortlicher über die Mittel.[263] Der individuelle gemeinsam Verantwortliche muss also nicht selbst Zugriff auf die verarbeiteten Daten oder die Verarbeitung haben, er muss die Verarbeitung allerdings mittels seiner Entscheidungsmacht kontrollieren können. Der Entbehrlichkeit des Zugriffs auf Daten bzw. Mittel widerspricht nicht, dass der Zugriff bei

[260] Vgl. BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 38 ff.

[261] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 69. Daher sei es a. denkbar, dass jemand gemeinsam Verantwortlicher sei ohne isoliert betrachtet Verantwortlicher zu sein: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 44.

[262] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 39.

[263] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 40.

wenigstens einem der gemeinsam Verantwortlichen entweder direkt oder via Auftragsverarbeiter vorliegen muss. Dies ist vielmehr Ausdruck der Arbeitsteilung unter gemeinsam Verantwortlichen. Würde man hingegen annehmen, der Zugriff auf Daten bzw. Mittel seitens aller gemeinsam Verantwortlichen sei erforderlich für eine gemeinsame Verantwortlichkeit, wäre dies ein Rückschritt von der organisatorisch-hierarchischen Zuweisung der Verantwortlichkeit hin zu einer technisch-bedingten und damit latent zufälligen Zuweisung. Gemeinsame Mittel setzen also nicht zwingend den Zugriff auf die Daten oder die Infrastruktur einer Verarbeitung voraus.

III. Rechtsprechung des EuGH

Untersucht man die jüngere Rechtsprechung des EuGH, so lagen in der Rechtssache Wirtschaftsakademie wie auch in Fashion ID gemeinsame Mittel im technischen Sinne anhand der Infrastruktur vor.[264] In der Rechtssache Wirtschaftsakademie war das gemeinsame Mittel die Fanpage, in Fashion ID das Social Plugin. In beiden Sachverhalten übernahm der Fanpage-Betreiber bzw. Websitebetreiber die Infrastruktur für die maßgeblichen Verarbeitungen insgesamt vom Plattformbetreiber. Dabei bestimmten die Fanpage und das Social Plugin, als Mittel im technischen Sinne, insgesamt die Elemente der Mittel, insbesondere die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen. Der Fanpage- bzw. Websitebetreiber machte sich diese Mittel zu eigen, indem er die Infrastruktur uneingeschränkt übernahm und für sich nutzte.[265] Für ein solches Zu-Eigen-Machen der Mittel ist kein Zugriff auf die Daten bzw. Mittel der Verarbeitung von Nöten. Sofern ein gemeinsam Verantwortlicher eine Verarbeitung ermöglicht, trägt er auch dasjenige Risiko, das sich aus einem fehlenden Zugriff auf die Daten bzw. Mittel entsteht. Auch im Bereich der Auftragsverarbeitung hat ein Verantwortlicher nicht unbedingt Zugriff hierauf. Er kann die Verarbeitung im Zweifel nur im Rahmen seiner Weisungen beeinflussen.

Dabei stellt sich aber die Frage, ob neben der Verwendung der Mittel noch ein weitergehender Einfluss auf die Mittel erforderlich ist, damit gemeinsame Mittel vorliegen.[266] Im Falle der Fanpage bestand seitens des Fanpage-Betreibers die Möglichkeit, die für die vom Plattformbetreiber zu erzeugende Besucherstatistik verwendeten Daten näher zu „parametrieren".[267] Diese Parametrierung bestimmte,

[264] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[265] Zum Begriff des Zu-Eigen-Machens: Kapitel 4 G. III. Zu-Eigen-Machen als Billigung oder Entscheidung?

[266] Für Ersteres wohl: Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 40.

[267] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36; a. *Hacker*, MMR 2018, 779, 779 f. ordnet dies als Mittel ein.

neben einem allgemeinen Einfluss auf die Verarbeitung, auch die Kategorien von betroffenen Personen, deren Daten verarbeitet werden sollten.[268] Die Parametrierung kann man somit als weitere Entscheidung über die wesentlichen Elemente der Mittel verstehen.[269] In der Rechtssache Fashion ID hatte der EuGH das Argument der „Parametrierung" allerdings nicht wieder aufgegriffen. Folglich ist die Ermöglichung der Verarbeitung in ihrer konkreten Form oder Identität, als deren entscheidende Beeinflussung, ausreichend für die Entscheidung über die Mittel.[270] Münzt man diese Ermöglichung auf die wesentlichen Elemente der Mittel um, könnte man darin zudem die Entscheidung über den Zugang zu den Daten erkennen. Festhalten lässt sich jedenfalls, dass in den Rechtssachen Wirtschaftsakademie wie Fashion ID eine gemeinsame Entscheidung über die Mittel wie auch gemeinsame Mittel als solche vorlagen. Ähnlich wie in den EuGH-Entscheidungen erkannte das LG Rostock auch für den Einsatz von Google Analytics im Rahmen einer Website auf gemeinsame Mittel.[271]

In der Rechtssache Jehovan todistajat[272] scheint im Gegensatz zu Wirtschaftsakademie und Fashion ID der Schwerpunkt des Urteils auf der Entscheidung über den Zweck zu liegen.[273] Dies ergibt sich aus dem Tenor des Urteils. So erfolge die Datenerhebung durch die verkündigenden Mitglieder. Die Gemeinschaft hingegen organisiere, koordiniere und ermuntere zur Verkündigungstätigkeit, also nicht der Verarbeitung als solcher. Der EuGH betont, dass die verkündigenden Mitglieder der Gemeinschaft, im Gegensatz zur Gemeinschaft, selbst entscheiden: „[...] unter welchen konkreten Umständen sie personenbezogene Daten über aufgesuchte Personen erheben, welche Daten sie genau erheben und auf welche Weise sie sie anschließend verarbeiten."[274] Maßgeblich sei daher der von der Gemeinschaft und den Mitgliedern geteilte Zweck der Verkündigungstätigkeit.[275] Dabei verklammert dieser Zweck, ähnlich wie die Statistikerstellung in der Rechtssache Wirtschaftsakademie,[276]

[268] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36.
[269] Dazu: Kapitel 2 D. Mittel.
[270] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77 f.
[271] LG Rostock, Urteil vom 15.09.2020 – 3 O 762/19 = ZD 2021, 166, Rn. 66 ff. Vgl. a. den HmbBfDI, „Tätigkeitsbericht Datenschutz 2019", S. 127. Dazu die Kritik von *Piltz*, https://www.delege-data.de/2020/02/datenschutzbehoerde-hamburg-gemeinsame-verantwortlichkeit-beim-einsatz-von-google-analytics-in-der-standardeinstellung/ (abgerufen am 17.07.2024).
[272] Dazu: Kapitel 4 B. II. Jehovan todistajat.
[273] Der Sachverhalt bezüglich der Mittel der Verarbeitung scheint insoweit strittig: EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 73.
[274] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 70.
[275] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 70 f.
[276] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36 f.

die Vorgangsreihe zur Erstellung der Liste von Haushalten, die nicht mehr aufgesucht werden sollen, seitens der Gemeinde. Für die Entscheidung über die Mittel der Verarbeitung scheint es nicht ausschlaggebend zu sein, dass die Gemeinschaft die Verkündigungstätigkeit der Mitglieder, allerdings nicht die Datenverarbeitung spezifisch, organisiert, koordiniert und dazu ermuntert.[277] Dies dürfte vielmehr den gemeinsamen Zweck der Gemeinschaft und der verkündigenden Mitglieder bestätigen. Es liegen also trotz dieser Ermunterung[278] offenbar keine gemeinsamen Mittel vor. Andererseits kann man gerade in dieser Ermunterung eine Festlegung hinsichtlich der Art der personenbezogenen Daten sowie der Kategorien betroffener Personen erkennen.

IV. Position der Aufsichtsbehörden

1. Art. 29-Datenschutzgruppe

Die Art. 29-Datenschutzgruppe schien im WP 169 davon auszugehen, dass gemeinsame Mittel für eine gemeinsame Verantwortlichkeit ausreichend sind. Deutlich wurde dies an Beispiel 15[279] (Plattformen für die Verwaltung von Gesundheitsdaten). Dieses Beispiel behandelte eine Behörde, die eine nationale Schaltstelle zur Regelung des Austauschs von Patientendaten zwischen Gesundheitsdiensten einrichtet. Dabei ist die einrichtende Behörde für die Art der Verarbeitung und die Nutzung der personenbezogenen Daten verantwortlich. Aufgrund der Vielzahl der beteiligten Gesundheitsdienste, die jeweils Verantwortliche darstellen sollen, sei es für die betroffenen Personen bzw. Patienten unklar, wer konkret Verantwortlicher ist. Daher sei jedenfalls die einrichtende Behörde Kontaktstelle für die betroffenen Person wie auch gemeinsam Verantwortlicher mit den jeweils verantwortlichen Gesundheitsdiensten.

Unklar blieb in diesem Beispiel allerdings, ob die Entscheidung über die Art der Verarbeitung und die Nutzung der Daten allein ausreichend für die gemeinsame Verantwortlichkeit der Behörde war oder ob daneben der Mangel an Transparenz für die betroffenen Personen eine weitere Voraussetzung sein sollte. Dabei wies die Art. 29-Datenschutzgruppe vor dem Beispiel darauf hin, dass eine größere Zahl von

[277] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 71.

[278] Anhand der Anleitung zum Verfassen der Notizen, der Erstellung der Verkündigungsbezirke und der „Verbotsliste“: EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 16 f., 22.

[279] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 29.

Verantwortlichen zu einer unerwünschten Komplexität und zu einer mangelnden Klarheit bei der Zuweisung der Verantwortung führen könnte.[280] Letzteres würde das Risiko bergen, dass die gesamte Verarbeitung aufgrund mangelnder Transparenz unrechtmäßig wäre. Diese mangelnde Transparenz würde den Grundsatz der Verarbeitung nach Treu und Glauben verletzen. Zudem ließe sich argumentieren, dass alle Beteiligten immer dann gesamtschuldnerisch haften sollten, wenn Unklarheiten hinsichtlich der Zuweisung der Verantwortung beständen.[281] Die Art. 29-Datenschutzgruppe deutete also scheinbar an, dass sich die gemeinsame Verantwortlichkeit auch aus dem Transparenz-Grundsatz in Art. 5 Abs. 1 lit. a DSGVO ergeben könnte. Die Begründung einer gemeinsamen Verantwortlichkeit allein aus fehlender Transparenz der tatsächlichen Verantwortlichkeit lässt sich aber nicht mit der Definition der gemeinsam Verantwortlichen und dem Erfordernis einer gemeinsamen Entscheidung vereinbaren und ist deswegen abzulehnen. Der Erkenntnisgewinn hinsichtlich gemeinsamer Mittel blieb in diesem Beispiel aufgrund der Erwägungen zur Transparenz insgesamt beschränkt.

2. Europäischer Datenschutzausschuss (EDPB)

Der EDPB wiederum setzt für eine gemeinsame Entscheidung über die Mittel zunächst nur voraus, dass zwei oder mehr Akteure Einfluss auf die Mittel der Verarbeitung ausüben.[282] Dabei sollen nicht alle Akteure über alle Aspekte der Mittel entscheiden müssen. Die Möglichkeit Elemente der Mittel zu beeinflussen sei schließlich auch von der (Verhandlungs-)Position eines gemeinsam Verantwortlichen abhängig. Wenn ein Akteur die Mittel für eine Verarbeitung bereitstelle und ein anderer Akteur diese einsetze, reiche dies für eine gemeinsame Entscheidung über die Mittel bereits aus.[283] Dabei verweist der EDPB explizit auf Plattformen, standardisierte Tools und andere Infrastruktur, die den Akteuren erlauben dieselben personenbezogenen Daten zu verarbeiten und

[280] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 29.

[281] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 30.

[282] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 63.

[283] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 64.

die so bereitgestellt werden, dass auch andere über die Art ihrer Verwendung entscheiden können.[284] Solange die Nutzer von solchen technischen Systemen also über die Verarbeitung personenbezogener Daten im Rahmen der Verwendung dieser Systeme entscheiden können, sei es unschädlich, dass die Systeme als fertiges Produkt verfügbar sind. Beispielhaft für ein solch technisches System und die Art der Verwendung sei in der Entscheidung Wirtschaftsakademie die Möglichkeit der „Parametrierung" der Fanpage hinsichtlich einer Zielgruppe.[285] Ebenso sei in der Rechtssache Fashion ID ein entscheidender Einfluss auf die Verarbeitung durch die Einbindung des Social Plugins ausgeübt worden.[286] Allerdings bedinge die Verwendung eines gemeinsamen Verarbeitungssystems oder einer Infrastruktur nicht zwangsläufig eine gemeinsame Verantwortlichkeit. So etwa dann nicht, wenn die Verarbeitung abtrennbar sei und von einem Akteur ohne Einmischung eines anderen Akteurs durchgeführt werden könne.[287]

3. Beispiele

Paradigmatisch für gemeinsame Mittel sei Beispiel 8[288] (Reisebüro (2)) in WP 169. In diesem Szenario beschließen ein Reisebüro, ein Hotel und eine Fluggesellschaft eine gemeinsame (internetgestützte) Buchungsplattform einzurichten. Sie vereinbaren wesentliche Elemente der Mittel, wie etwa welche Daten gespeichert werden, wie Reservierungen zugewiesen und bestätigt werden und wer Zugang zu den Daten haben soll. Zusätzlich wollen sie ihre Kundendaten gemeinsam nutzen, um Werbeaktionen durchzuführen. Alle Beteiligten sollen damit einen Entscheidungsbeitrag hinsichtlich der wesentlichen Mittel im Rahmen der Verarbeitungen über die Plattform erbracht haben. Wie sich aus dem vorhergehenden Absatz erschließt, ging die Art. 29-Datenschutzgruppe in so einem Fall von einer gemeinsamen Verantwortlichkeit aus, auch bei potenziell divergierenden Zwecken.[289] Die gemeinsame Verantwortlichkeit

[284] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 65.

[285] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 66.

[286] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 67.

[287] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68.

[288] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 1 Reisebüro.

[289] Insofern ist die Schlussfolgerung von *Kartheuser/Nabulsi*, MMR 2018, 717, 719 hinsichtlich der

bestünde allerdings nicht für Verarbeitungen der Beteiligten außerhalb der Plattform. In den Leitlinien des EDPB verfolgen dieselben Akteure zusätzlich den gemeinsamen Zweck von Reisepaketangeboten. Inwiefern nach Ansicht des EDPB die Entscheidung nur über die gemeinsamen Mittel also weiterhin für eine gemeinsame Verantwortlichkeit ausreichen soll, erscheint daher fraglich.

Auch Forschungsinstitute, welche die bereits vorhandene Plattform eines beteiligten Instituts für ein gemeinsames Forschungsprojekt nutzen, sollen als gemeinsam Verantwortliche gelten.[290] Dies sei dadurch begründet, dass jedes beteiligte Forschungsinstitut personenbezogene Daten in die Plattform für die Zwecke der gemeinsamen Forschung einspeise und wiederum die Daten von anderen nutze, um Forschung zu betreiben. Aufgrund der Einigung der beteiligten Forschungsinstitute auf den Zweck und die dafür zu verwendenden Mittel – die vorhandene Plattform – bestehe eine gemeinsame Verantwortlichkeit für die Speicherung und Bereitstellung der Daten auf der Plattform. Außerhalb der Verarbeitung auf der Plattform bestehe keine gemeinsame Verantwortlichkeit der Forschungsinstitute im Rahmen derer jeweiligen Zwecke.

Ein weiteres Beispiel für gemeinsam Verantwortliche soll in der Organisation eines Marketingevents für ein gemeinsam entwickeltes Produkt zweier Unternehmen bestehen.[291] Diese teilen die Daten in ihren jeweilige Kunden- und Interessenten-Datenbanken und entscheiden über die Einladungsliste für das Event auf Basis der geteilten Daten. Ebenso legen sie die Modalitäten für die Versendung der Einladungen fest und wie Feedback im Rahmen des Events und in den darauf folgenden Marketingaktionen berücksichtigt werden soll. Folglich seien beide Unternehmen gemeinsam Verantwortliche für die Organisation des Marketingevents.

Auch die Durchführung klinischer Studien könne je nach Sachverhalt eine gemeinsame Verantwortlichkeit begründen. Nach dem Beispiel des EDPB entscheiden sich ein Gesundheitspflegedienstleister und eine Universität eine klinische Studie mit demselben Zweck durchzuführen.[292] Sie arbeiten dabei im Rahmen des Entwurfs des

---

Vorgangsreihe in Bezug auf einen gemeinsamen Zweck falsch. Die Vorgangsreihe muss aus Sicht der Verantwortlichen als einheitlich zu bewerten sein, nicht aus Sicht der betroffenen Person. Die Buchungsplattform wird zur Vereinfachung von Buchungen, nicht zur Ermöglichung konkreter Reisen eingerichtet. Es handelt sich bei der Plattform somit nur um ein gemeinsames Mittel. Der Zweck der Plattform hat nichts mit dem der Verarbeitung zu tun.

[290] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 2 Forschungsprojekte von Institutionen. Hierzu auch: *Hessel/Leicht*, DuD 2022, 305.

[291] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 3 Marketingkampagne.

[292] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor

Studienprotokolls zusammen und legen etwa Zweck, Methodologie/Design der Studie, die Daten die erhoben werden, Ein- und Ausschluss-Kriterien von Studienteilnehmern sowie die Wiederverwendung von Datenbanken fest. Dabei sei aber die Erhebung der personenbezogenen Daten für die Studie von der Verwendung für die Patientenpflege abzugrenzen. Bei letzterem bleibe der Dienstleister singulärer Verantwortlicher. Sollte der Dienstleister nicht das Studienprotokoll zusammen mit der Universität festlegen, sondern nur diese allein, sei er Auftragsverarbeiter und nicht gemeinsam Verantwortlicher.

Neben diesen Positivbeispielen für gemeinsame Verantwortlichkeit und dabei vor allem für gemeinsame Mittel, stellt der EDPB aber auch Szenarien vor, in denen keine gemeinsame Verantwortlichkeit, trotz einer geteilten Datenbank oder gemeinsamer Infrastruktur, vorliegen soll. Maßgeblich sei dabei, dass jeder Akteur seine Zwecke unabhängig festlege.[293] So soll etwa bei einer Unternehmensgruppe, die eine einheitliche Datenbank für das Management von Kunden und Interessenten nutzt, dann keine gemeinsame Verantwortlichkeit vorliegen, wenn die Muttergesellschaft für das Hosting der Datenbank als Auftragsverarbeiter fungiert und die einzelnen Unternehmen nur eigene Daten eingeben und für eigene Zwecke verarbeiten.[294] Dabei soll jeder Akteur (scheinbar also jedes Unternehmen) unabhängig über den Zugang, die Speicherdauer, sowie die Berichtigung und Änderung der Daten entscheiden können. Die einzelnen Unternehmen sollen zudem untereinander nicht die jeweils anderen Daten abrufen oder nutzen können. Unter diesen Umständen soll die bloße Nutzung einer gemeinsamen Datenbank noch keine gemeinsame Verantwortlichkeit begründen. In Verbindung mit der Auftragsverarbeitung durch die Muttergesellschaft wäre jedes Unternehmen singulärer Verantwortlicher.

Ebenso soll auch dann keine gemeinsame Verantwortlichkeit vorliegen, wenn ein Unternehmen Z eine Datenbank hoste und für andere Unternehmen zur Verarbeitung und zum Hosting von personenbezogenen Daten über deren Arbeitnehmer

in the GDPR, 07.07.2021, Rn. 68 Beispiel 4 Klinische Studien. Vgl. a. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 36 f. Beispiel 25.

[293] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 71. Dies scheint mit der Fallgruppe der „converging decisions" (dazu: Kapitel 4 H. III. 4. c) Europäischer Datenschutzausschuss (EDPB)) in einem gewissen Widerspruch zu stehen.

[294] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 71 Beispiel 1. Dieses Beispiel erinnert an *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 26 Beispiel 11 (E-Government-Portale).

bereitstellt.[295] Solange das Hosting dieser Daten auf Weisung der anderen Unternehmen erfolge, sei Unternehmen Z für die Verarbeitung und die Speicherung (damit ist wohl das Hosting der Daten, nicht der Datenbank gemeint) nur Auftragsverarbeiter. Dies gelte jedenfalls soweit die Unternehmen die Daten ohne Einmischung von Z verarbeiteten und sie mit Z keine Zwecken teilen würden.

V. Fazit

Im Rahmen der Rechtsprechung des EuGH und der Ausführungen der Aufsichtsbehörden lässt sich erkennen, dass gemeinsame Mittel den Regelfall einer gemeinsamen Verantwortlichkeit darstellen. Versteht man die Entscheidung über die Art personenbezogener Daten sowie die Kategorien betroffener Personen als Identitätsgarant für das gemeinsame Bezugsobjekt einer Verarbeitung zwischen gemeinsam Verantwortlichen,[296] müssen also zumindest insoweit gemeinsame Mittel vorliegen. Obwohl der EDPB auf dieses Erfordernis nicht explizit hinweist, deckt sich dies mit seinen Beispielen. Abseits der Garantie einer einheitlichen Verarbeitung können die Mittel zwischen den gemeinsam Verantwortlichen aber durchaus divergieren.

G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung

Bei gemeinsam Verantwortlichen stellt sich als Konsequenz der bisherigen Erwägungen die Frage, inwiefern diese divergierende Zwecke oder Mittel billigen oder jedenfalls nicht missbilligen müssen.[297] Die Billigung[298] ist dabei als Handlung eines gemeinsam Verantwortlichen zu verstehen, die wenigstens implizit eine Anerkennung der oder Gleichgültigkeit gegenüber den divergierenden Zwecken oder Mitteln der anderen gemeinsam Verantwortlichen bedeutet.[299] Dabei muss in irgendeiner Art und Weise ersichtlich sein, dass ein gemeinsam Verantwortlicher mit den divergierenden Zwecken oder Mitteln anderer gemeinsam Verantwortlicher einverstanden ist. Dieses

[295] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 71 Beispiel 2.

[296] Dazu: Kapitel 4 H. II. Gemeinsame Zwecke oder Mittel als Identitätsgarant der Verarbeitung.

[297] Vgl. zum Begriff Entscheidung Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 13.

[298] Vgl. zur Billigung Ehmann/Selmayr/*Klabunde/Horvath*, Art. 4 DS-GVO, Rn. 26.

[299] Vgl. die Analyse der Rechtssache Fashion ID bei *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 64 ff.

Einverständnis kann man regelmäßig in der weiteren Durchführung der Verarbeitung erkennen. Denkbar ist allerdings auch, dass eine solche Billigung nur explizit erfolgen kann. Ein gemeinsam Verantwortlicher müsste dann also ausdrücklich, etwa in einer Vereinbarung, sein Einverständnis mit den ihm fremden Zwecken oder Mitteln erklären. In jedem Fall muss der Billigung aber eine Verarbeitung folgen, damit die Billigung eine Konsequenz für die Verarbeitung i.S.d. Definitionselements der Entscheidung erlangt. Die Billigung kompensiert also insgesamt die Divergenz der Zwecke oder Mittel zwischen den gemeinsam Verantwortlichen.[300] Sie ersetzt also etwa einen gemeinsamen Zweck.

Diese Billigung muss aufgrund des Definitionselements der Entscheidung zudem eine Entscheidungsqualität aufweisen. Billigt ein Akteur die Zwecke eines anderen Verantwortlichen, aber handelt er weisungsabhängig, so ist er entweder Auftragsverarbeiter oder Teil des Verantwortlichen. Streng genommen liegt dann bereits keine Billigung vor, da diese einen Entscheidungsspielraum, also zumindest die Möglichkeit der Nicht-Billigung voraussetzen würde. Die Billigung oder Nicht-Billigung wird dann gewissermaßen von der Weisungsabhängigkeit überschrieben. Setzt ein Akteur hingegen eigene Zwecke, so ist er Verantwortlicher, wie sich aus Art. 28 Abs. 10 DSGVO für den Auftragsverarbeiter und im Rahmen eines Erst-Recht-Schlusses auch für dem Verantwortlichen Untergeordnete ergibt.[301] Werden diese Zwecke von anderen Verantwortlichen gebilligt, so bilden sie, jedenfalls im Hinblick auf das Element der Entscheidung über die Zwecke, potenziell gemeinsam Verantwortliche.[302]

Zunächst stellen sich die Fragen, ob eine Billigung notwendig ist, wie sie verhindert werden kann und worauf sie sich beziehen muss. Daneben stellt sich die Frage, wie ein Zu-Eigen-Machen fremder Zwecke im Verhältnis zur Billigung zu werten ist. Ebenso ist zu hinterfragen, ob eine Billigung auch hinsichtlich der Mittel vorliegen kann oder muss. Zuletzt wird der Stellenwert der Billigung erörtert.

Ausgehend von der Prämisse, dass jeweils eigene Zwecke ausreichend für eine gemeinsame Verantwortlichkeit sind, sofern gemeinsame Mittel vorliegen,[303] muss eine Billigung der fremden Zwecke zwingend erforderlich sein, damit einem Verantwortlichen eine gemeinsame Verantwortlichkeit nicht aufgezwungen werden

[300] Dazu: Kapitel 4 H. III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung.

[301] Dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[302] Vgl. Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 24.

[303] Dazu: Kapitel 4 H. III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung.

kann.[304] Eine implizite Billigung kann dann angenommen werden, wenn zwischen gemeinsam Verantwortlichen Zweckkomplementarität[305] vorliegt und die Verarbeitung durchgeführt wird.[306] Zweckkomplementarität ist dann gegeben, wenn zwischen gemeinsam Verantwortlichen zwar divergierende Zwecke vorliegen, diese Zwecke aber im wechselseitigen Interesse sind, etwa im Rahmen eines Austauschverhältnisses. Dabei kann sich das wechselseitige Interesse in Ermangelung expliziter Manifestation auch aus den tatsächlichen Umständen begründen. Die Zweckkomplementarität ist allerdings zunächst nur ein Indiz dafür, dass eine Billigung möglich ist. Daher ist daneben noch eine Handlung notwendig, die den Willen zur Zusammenarbeit ausdrückt. Zu denken ist hier etwa an die Einrichtung einer gemeinsamen Plattform zur Verwaltung von Reisereservierungen zwischen einem Reisebüro, einer Hotelkette und einer Fluggesellschaft.[307] Insgesamt besteht, sofern gemeinsame Mittel vorhanden sind, durch die implizierte Billigung eine gemeinsame Entscheidung über Zwecke und Mittel. Ersichtlich ist das Konzept der Zweckkomplementarität in den Rechtssachen Wirtschaftsakademie sowie Fashion ID.[308] Hier lagen jeweils unterschiedliche Zwecke zwischen dem Plattformbetreiber und dem Fanpage- bzw. Websitebetreiber vor.[309] Eine Billigung thematisierte der EuGH zwar nicht ausdrücklich, allerdings ergibt sich diese zwangsläufig aus der Zweckkomplementarität und der weiteren Durchführung der Verarbeitung. Eine explizite Billigung ist also im Hinblick auf die Rechtsprechung des EuGH nicht notwendig. Eine explizite Billigung vorauszusetzen würde daneben auch eine Förmelei bedeuten. Denn diese explizite Billigung müsste entweder mündlich oder schriftlich

[304] In diese Richtung wohl: Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 9; möglicherweise a. *Kartheuser/Nabulsi*, MMR 2018, 717, 720, die ein „über die Details der Verarbeitungsvorgänge im Bilde sein" fordern. Anders *Moos/Rothkegel*, MMR 2019, 584, 585, die zwar eine Billigung ausreichen lassen, für diese aber einen gemeinsamen Zweck verlangen.

[305] Dazu: Kapitel 4 E. I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen.

[306] Anders *Lezzi/Oberlin*, ZD 2018, 398, 400, die eine absichtliche Zusammenarbeit voraussetzen. Unklar Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 12, aber mit Tendenz zur bewussten Zusammenarbeit.

[307] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24 Beispiel 8.

[308] Vgl. die Feststellung bei *Hanloser*, ZD 2019, 455, 459, dass keine Willenseinigung oder ein konsensuales Band zwischen den gemeinsam Verantwortlichen erforderlich wäre.

[309] In der Rechtssache Wirtschaftsakademie auf Seiten der Plattform: Verbesserung des Werbungssystems, auf Seiten des Fanpage-Betreibers: bessere Vermarktung anhand der Statistik (EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34). In der Rechtssache Fashion ID auf Seiten der Plattform: Verfügung über Daten zu eigenen Zwecken, auf Seiten des Websitebetreibers: bessere Sichtbarkeit/Vermarktung (EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80).

erfolgen. Eine mündliche Billigung wäre kaum nachzuvollziehen. Eine schriftliche Billigung hingegen würde neben der Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO eine weitere Vereinbarung voraussetzen. Der Notwendigkeit einer Vereinbarung über die Zwecke und Mittel einer Verarbeitung hat der EuGH aber in der Rechtssache NZÖG eine ausdrückliche Absage erteilt.[310] Ein Festhalten der Billigung in der Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO wiederum wäre nur dann denkbar, wenn vor der tatsächlichen Verarbeitung bereits die Vereinbarung geschlossen würde. Denn die Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO ist Folge und gerade nicht Voraussetzung der gemeinsamen Verantwortlichkeit ist. Selbst bei einer expliziten Billigung wäre zudem immer noch zu fordern, dass die Verarbeitung dann auch tatsächlich durchgeführt wird, da sonst die Billigung keinerlei Konsequenz für die Verarbeitung im Sinne einer Entscheidung hätte. Dies wird anhand der Rechtssache NZÖG deutlich. Dort hatte der EuGH entschieden, dass sich ein Verantwortlicher nur dann von seiner Verantwortlichkeit für eine von ihm mitgeprägte Verarbeitung erfolgreich distanzieren kann, wenn er der Verarbeitung ausdrücklich widerspreche.[311] Nur dann könne davon ausgegangen werden, dass die Verarbeitung nicht in seinem Namen erfolge.

Entbehrlich ist eine Billigung dann, wenn ein gemeinsamer Zweck aufgrund einer Einigung der gemeinsam Verantwortlichen vorliegt. Denn dann liegt bereits keine Divergenz der Zwecke vor. Dies war etwa der Fall in dem Urteil des EuGH in der Rechtssache Jehovan todistajat, in der Glaubensgemeinschaft und Mitglieder den gemeinsamen Zweck der Verkündigungstätigkeit verfolgten.[312]

Unerheblich ist für die Billigung, ob andere potenziell gemeinsam Verantwortliche einem Verantwortlichen individuell bekannt sind.[313] Deutlich wird dies insbesondere bei antizipierten gemeinsamen Verantwortlichkeiten durch Bereitstellung eines Angebots wie in den Rechtssachen Wirtschaftsakademie und Fashion ID. Ebenso unerheblich sind die Annahmen eines Verantwortlichen, welche Verantwortlichkeitsrolle ein anderer Akteur wahrnimmt. Sofern eine Zusammenarbeit erwünscht ist und sich aus den tatsächlichen Umständen eine Rolle als gemeinsam Verantwortlicher ergibt, ist eine anderweitige Fehlvorstellung unerheblich. Dies gilt

[310] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 44.

[311] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 37

[312] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 44, 71.

[313] Vgl. zu akuter Kenntnis *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 44. Kritisch: *Moos/Rothkegel*, MMR 2019, 584, 585.

etwa für den Fall, dass ausdrücklich eine Auftragsverarbeitung vereinbart wird, tatsächlich aber, aufgrund der Sachlage, eine gemeinsame Verantwortlichkeit vorliegt.

I. Verhinderung einer impliziten Billigung

Soweit eine implizite Billigung ausreicht, stellt sich die Frage, wie ein Verantwortlicher diese, abseits des erwähnten ausdrücklichen Widerspruchs, verhindern kann. Bedeutsam wird eine Verhinderung insbesondere dann, wenn ein Akteur eine gemeinsame Verantwortlichkeit antizipiert und andere Akteure ein solches Angebot nur noch wahrnehmen müssen. Es geht also um die Kategorie einer Art gemeinsamen Verantwortlichkeit „ad personas incertas". Zur Veranschaulichung kann wiederum auf die Urteile des EuGH[314] in den Rechtssachen Wirtschaftsakademie und Fashion ID zurückgegriffen werden. In beiden Sachverhalten lag ein vorgefertigtes Angebot durch den Plattformbetreiber vor. Der Fanpage-Betreiber bzw. Websitebetreiber musste nur dieses Angebot nutzen. Ein individueller Verhandlungsprozess über die Einzelheiten der Verarbeitung war nicht möglich. Unter die Wirkung einer impliziten Billigung fällt zudem ein „rogue processor"[315], der im Rahmen einer eigenen Zweckentscheidung nicht singulärer, sondern gemeinsam Verantwortlicher wäre.

Will ein Verantwortlicher in solchen Sachverhalten die Vermutung einer impliziten Billigung vorbeugen, muss er durch entsprechende Vereinbarungen oder technische und organisatorische Maßnahmen sicherstellen,[316] dass eine Billigung der Zwecke der anderen Verantwortlichen gerade nicht angenommen werden kann.[317] Dies kann neben einem ausdrücklichen Widerspruch[318] etwa durch Nutzungsbedingungen zu den zur Verfügung gestellten Daten bzw. Mitteln erfolgen. Daneben sind als technische Maßnahmen digitale Wasserzeichen der Daten oder API-Beschränkungen[319] denkbar.

---

[314] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[315] Also ein ehemaliger Auftragsverarbeiter, der Auftragsverarbeiterexzess begangen hat.

[316] Vgl. zu technischen Sicherheitsmaßnahmen und Verantwortung im Zusammenhang mit dem Mitarbeiterexzess *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20 sowie ebd., 21 Beispiel 4.

[317] Vgl. *Jung/Hansch*, ZD 2019, 143, 145; ähnlich: Plath/*Plath*, Art. 26 DSGVO, Rn. 9 f.; *Hessel/Potel*, K&R 2020, 654, 656. Vgl. insofern die Kritik der antizipierten gemeinsamen Verantwortlichkeit bei *Moos/Rothkegel*, MMR 2019, 584, 585 f., die aber a. einen gemeinsamen Zweck voraussetzen.

[318] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 37.

[319] Vgl. hierzu *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 57 ff.

II. Vorgang und Vorgangsreihe als Bezugsobjekt der Billigung

Ebenso wie bei der Entscheidung insgesamt ist Objekt der Billigung immer nur der konkrete Verarbeitungsvorgang bzw. die Vorgangsreihe. Billigt ein gemeinsam Verantwortlicher also etwa die Zwecke der nachgelagerten Verarbeitungen eines anderen gemeinsam Verantwortlichen nicht, muss er gegebenenfalls die diesem vorgelagerte gemeinsam verantwortete Verarbeitung verhindern. Denn dem Verantwortlichen steht es frei, für die gemeinsam verantworteten Verarbeitungen die Billigung der Zwecke des anderen gemeinsam Verantwortlichen durch entsprechende Maßnahmen zu verweigern und so nachgelagerte Verarbeitungen zu verhindern. Sofern ein gemeinsam Verantwortlicher also die Zwecke der anderen gemeinsam Verantwortlichen in Bezug auf nachgelagerte Verarbeitungen missbilligt, die dafür ursächliche, vorgelagerte Verarbeitung aber billigt, ist dies somit insgesamt ausreichend für eine Billigung dieser damit gemeinsam verantworteten vorgelagerten Verarbeitung.

So wäre es etwa in der Rechtssache Fashion ID unbeachtlich, wenn der Websitebetreiber zwar die Erhebung der Daten mittels des Social Plugins durch den Plattformbetreiber billigen würde, die daran anschließenden Verarbeitungen, etwa zum Profiling, hingegen missbillige.[320] Denn für die nachgelagerte Verarbeitung besteht ohnehin, auch bei einer Billigung durch den Websitebetreiber, keine gemeinsame Verantwortlichkeit mehr.

Die Billigung entfaltet insbesondere im Rahmen von Vorgangsreihen Relevanz, in denen zwar einzelne Verarbeitungsvorgänge isoliert nicht den Zwecken eines gemeinsam Verantwortlichen dienen, diese Vorgänge gleichsam aber notwendige Vorbedingung zu den seinen Zwecken entsprechenden Vorgängen darstellen. Deutlich wird dies in der Rechtssache Wirtschaftsakademie.[321] Zwar mag der Fanpage-Betreiber kein isoliertes Interesse nur an der Erhebung der Besucherdaten der Fanpage haben, allerdings bildet diese Erhebung notwendigerweise die Voraussetzung für den späteren Erhalt der Statistiken über die Besucher der Fanpage. Während der Plattformbetreiber mit den verschiedenen Verarbeitungsvorgängen unterschiedliche Zwecke verfolgen wird, werden sie für den Fanpage-Betreiber durch seinen Zweck des Erhalts der Statistik zu einer Vorgangsreihe verklammert. Er muss, will er diese Statistik erhalten, also die der Erstellung der Statistik vorgelagerten Verarbeitungsvorgänge billigen. Deutlich wird in diesem Sachverhalt zudem, dass die Bestimmung von Vorgangsreihen für die

[320] Hierbei handelt es sich nicht zwangsläufig um ein widersprüchliches Verhalten, da dem gemeinsam Verantwortlichen die Folgezwecke nicht notwendigerweise bekannt sind.

[321] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34, 36, 39.

Verantwortlichen individuell vorgenommen werden muss, eben aufgrund der individuellen Klammerwirkung des jeweils verfolgten Zweckes.[322]

Auch die Billigung zieht daher notwendigerweise eine Kleinteiligkeit der Analyse der Verarbeitungsvorgänge nach sich. Sie ist aber gegenüber der Bildung übergeordneter Zweckebenen oder von Makrozwecken verschiedener gemeinsam Verantwortlicher im Sinne einer Zweckeinheit[323] vorzugswürdig. Denn das Konzept einer solchen Zweckeinheit widerspricht dem Grundsatz der Zweckbindung in Form der Zweckfestlegung in Art. 5 Abs. 1 lit. b DSGVO und ist der Rechtssicherheit insgesamt nicht förderlich.[324]

III. Zu-Eigen-Machen als Billigung oder Entscheidung?

Billigt ein Akteur nicht nur fremde Zwecke oder Mittel, sondern macht er sie sich zu eigen, stellt sich die Frage, wie dies einzuordnen ist. Dabei stellt ein Zu-Eigen-Machen die uneingeschränkte Übernahme der Zwecke oder Mittel eines Verantwortlichen durch einen Akteur dar. Das Zu-Eigen-Machen ist also so zu verstehen, dass es das Fehlen eines eigenen Entscheidungsbeitrags zur Verarbeitung kompensiert, während die Billigung divergierende Zwecke oder Mittel kompensiert.

Maßgeblich ist beim Zu-Eigen-Machen zunächst, damit es sich überhaupt um einen Entscheidungsbeitrag handeln kann, ob der Akteur einen Entscheidungsspielraum im Hinblick auf die Zwecke oder wesentlichen Elemente der Mittel hat. Sofern ein Akteur die Möglichkeit hat, sich die Zwecke oder wesentlichen Elemente der Mittel eines anderen Verantwortlichen auch nicht zu eigen zu machen, besteht in der Wahrnehmung dieses Entscheidungsspielraums notwendigerweise eine Entscheidung. Das Zu-Eigen-Machen muss allerdings durch Umstände indiziert sein, die über eine reine Hinnahme der fremden Zwecke oder wesentlichen Elemente der Mittel hinausgehen.[325] Diese sind in einem aktiven Tun, bei den Mitteln regelmäßig in der Durchführung der Verarbeitung als implizites Zu-Eigen-Machen zu erkennen.

Ginge man davon aus, dass ein reines Zu-Eigen-Machen fremder Zwecke nicht ausreichend wäre für eine Entscheidung über die Zwecke, würde dies im

[322] Dazu: Kapitel 4 D. Die Verarbeitung als Vorgangsreihe bei gemeinsam Verantwortlichen.

[323] So: EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 105.

[324] Kritisch zur Begründung des EuGH in Wirtschaftsakademie insofern: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 44. Ähnlich wohl a.: *Datenschutzkonferenz*, Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, 19.03.2018, 3 im Hinblick auf den Anschluss an im Voraus festgelegte Zwecke und Mittel.

[325] So wie etwa die Verbreitung des Glaubens in: EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 70.

Umkehrschluss bedeuten, dass in Szenarien mit mehreren Verantwortlichen, die einen gemeinsamen Zweck verfolgen, regelmäßig keine gemeinsame Verantwortlichkeit bestünde, da es an einer eigenen Entscheidung der Beteiligten fehlen würde. Ein gemeinsamer Zweck entsteht häufig nicht notwendigerweise erst im Verhandlungsprozess der Verantwortlichen, sondern wird bestenfalls als verhandelbar von einer Partei gesetzt. Eine Verhandelbarkeit des Zweckes[326] und damit ein potenzieller Einfluss auf diesen wäre also häufig eine Förmelei. Daher reicht allein aus pragmatischer Sicht ein Zu-Eigen-Machen für eine Entscheidung aus.[327] Denn bei dem Zu-Eigen-Machen fremder Zwecke handelt es sich schlussendlich um die Entscheidung über einen gemeinsamen Zweck. Folglich handelt es sich beim Zu-Eigen-Machen auch nicht mehr um eine Billigung. Die gleichen Erwägungen gelten auch für das Zu-Eigen-Machen fremder Mittel. Denkbar ist ein solches Zu-Eigen-Machen fremder Mittel etwa im Rahmen eines späteren Anschlusses an ein Joint-Venture oder ein Forschungsprojekt.

IV. Die Billigung von fremden Mitteln

Eine Billigung fremder Mittel ist ebenso wie die Billigung fremder Zwecke grundsätzlich denkbar. Dabei muss allerdings zunächst die Identität der Verarbeitung zwischen den gemeinsam Verantwortlichen sichergestellt werden. Die Identität der Verarbeitung betrifft vor allem die Frage, welche personenbezogenen Daten überhaupt verarbeitet werden. Die verarbeiteten Daten sind wiederum Teil der Entscheidung über die wesentlichen Elemente der Mittel, die ein Verantwortlicher treffen muss. Anhand der zu verarbeitenden Daten lässt sich der Verarbeitungsvorgang bzw. die Vorgangsreihe erst sinnvoll konturieren.

Die für die Entscheidung maßgeblichen Verarbeitungsvorgänge müssen also dieselben zwischen den verschiedenen gemeinsam Verantwortlichen sein. Unproblematisch ist dies etwa bei gemeinsamen Datenpools oder der arbeitsteiligen Verarbeitung unter einem gemeinsamen Zweck. Bei Letzterem kann die Vorgangsreihe eine zusätzliche Klammerwirkung entfalten, die die Identität der Verarbeitung sicherstellt. Sind die für die Verantwortlichkeit maßgeblichen Vorgänge allerdings bereits völlig unterschiedliche, lassen sich diese „fremden Mittel" nicht mehr durch eine Billigung kompensieren. Denn es liegt bereits nicht mehr eine Entscheidung über die Mittel derselben Verarbeitung vor. Sind die maßgeblichen Verarbeitungsvorgänge

[326] Etwa im Sinne der „consideration" im Common Law.
[327] Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 143 f.

hingegen identisch, lassen sich divergierende Mittel, etwa im Hinblick auf technische und organisatorische Fragen durchaus billigen. Gleiches gilt auch für die wesentlichen Elemente der Mittel, solange diese nicht die Identität der Verarbeitung tangieren. Liegt aber kein Zu-Eigen-Machen der Mittel vor, muss wenigstens ein gemeinsamer Zweck vorliegen, damit eine gemeinsame Entscheidung besteht.[328]

Eine Billigung fremder Mittel ist dann nicht erforderlich, wenn ein Zu-Eigen-Machen der Mittel vorliegt. Beispielhaft hierfür ist das Urteil in der Rechtssache Jehovan todistajat.[329] Dort hatte sich die Glaubensgemeinschaft die Aufzeichnungen ihrer Mitglieder im Rahmen deren Verkündigungstätigkeit von Tür zu Tür zwecks Koordinierung und Organisation der Verkündigungstätigkeit zu eigen gemacht. Auch bei den Rechtssachen Wirtschaftsakademie sowie Fashion ID handelt es sich um ein Zu-Eigen-Machen der fremden Mittel. So lassen sich die Ausführungen des EuGH zu den Mitteln in der Rechtssache Fashion ID nur so interpretieren, dass ein Zu-Eigen-Machen der Mittel des anderen Akteurs, im Wissen um dessen Verarbeitung, als gemeinsame Entscheidung über die Mittel der Verarbeitung ausreicht.[330] Der Fanpage-Betreiber bzw. Websitebetreiber hatte in diesen Fällen nur die Möglichkeit, die Fanpage-Infrastruktur bzw. das Social Plugin so wie sie bzw. es bereitgestellt wurde zu verwenden.

Macht sich ein Akteur fremde Mittel in Unkenntnis bestimmter verarbeitungstechnischer Konsequenzen, also etwa des Datenflusses an einen weiteren Akteur, zu eigen, befreit ihn das nicht notwendigerweise von einer gemeinsamen Verantwortlichkeit. Ausreichend für eine Entscheidung über die Mittel ist, wie dargestellt,[331] ein Kennenmüssen. Sofern ein solcher Datenfluss im Rahmen der allgemeinen Sorgfaltspflichten erkennbar ist, wird der Akteur, auch bei tatsächlicher Unkenntnis, zum gemeinsam Verantwortlichen. Denkbar ist das Zu-Eigen-Machen fremder Mittel in Unkenntnis insbesondere im Fall von Programmbibliotheken.[332] Diese können häufig Übermittlungen beinhalten, die dem Verantwortlichen im Rahmen einer rudimentären Prüfung auffallen müssten. Will hingegen ein Akteur die Verwendung seiner Mittel durch Zu-Eigen-Machen anderer Akteure verhindern, so muss er entsprechende Vereinbarungen oder insbesondere auch technische und organisatorische Maßnahmen dagegen treffen. Zu denken ist hier insbesondere an die

[328] Dazu: Kapitel 4 H. II. Gemeinsame Zwecke oder Mittel als Identitätsgarant der Verarbeitung.
[329] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 70.
[330] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77.
[331] Dazu: Kapitel 2 E. I. 4. c) Notwendige Kenntniselemente und Kennenmüssen bei gemeinsam Verantwortlichen.
[332] Zu denken ist auch an sogenannte SDKs (Software-Development-Kits).

Nutzung von Programmierschnittstellen, sogenannten APIs, über die personenbezogene Daten abgerufen werden können.

V. Stellenwert der Billigung

Insgesamt stellt sich die Frage, welche Bedeutung die Billigung im Hinblick auf die Entscheidung hat. Die Billigung ist zunächst von dem Zu-Eigen-Machen zu unterscheiden. Das Zu-Eigen-Machen kompensiert das Fehlen eines eigenen Entscheidungsbeitrags zur Verarbeitung, während die Billigung divergierende Zwecke oder Mittel kompensiert. Dabei kann die Billigung im Rahmen der Zweckkomplementarität, abseits widersprechender faktischer Umstände, bei Durchführung der Verarbeitung impliziert werden. Die Billigung ist somit ein Mechanismus, der sicherstellt, dass trotz gewisser Divergenzen der gemeinsam Verantwortlichen diesen keine Verantwortlichkeit aufgezwungen wird. Als solcher ist er auch präziser als die Bildung eines systematisch, abseits der Vorgangsreihe, nicht angelegten übergeordneten Zweckes zwischen gemeinsam Verantwortlichen. Erfolgt die Billigung nicht explizit und kann sie auch im Rahmen einer impliziten Billigung nicht vermutet werden, entsteht keine gemeinsame Verantwortlichkeit bei divergierenden Zwecken oder Mitteln.[333]

Auch wenn die Billigung eine Entscheidung über die jeweils divergierenden Zwecke oder Mittel darstellt, kann sie nicht den Entscheidungsbeitrag eines gemeinsam Verantwortlichen überhaupt ersetzen.[334] Die bloße Billigung sowohl von Zwecken als auch Mitteln begründet daher keine gemeinsame Verantwortlichkeit. Erforderlich ist entweder ein eigener Entscheidungsbeitrag zu Zwecken oder Mitteln oder zumindest das Zu-Eigen-Machen der Zwecke oder Mittel eines anderen Verantwortlichen.[335]

H. Die gemeinsame Entscheidung

Wie festgestellt, sind isoliert betrachtet weder ein gemeinsamer Zweck noch gemeinsame Mittel, abseits der Identität der Verarbeitung, für eine gemeinsame

[333] Die beteiligten Akteure bleiben dann separat verantwortlich, sofern die Voraussetzungen dafür vorliegen.

[334] Ähnlich wohl *Monreal*, CR 2019, 797, Rn. 40, der keine explizite Einigung gemeinsam Verantwortlicher, wohl aber einen Beitrag verlangt. Kritisch bezüglich der reinen Billigung eines Zwecks: *Kartheuser/Nabulsi*, MMR 2018, 717, 719 zu *Datenschutzkonferenz*, Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, 19.03.2018, 3.

[335] Dazu: Kapitel 4 H. I. Die reine Billigung von Zwecken und Mitteln als gemeinsame Entscheidung?

Verantwortlichkeit erforderlich. Daran anschließend stellt sich aber die Frage, ob weder gemeinsame Zwecke noch gemeinsame Mittel für eine gemeinsame Entscheidung notwendig sind oder ob diese wenigstens alternativ vorliegen müssen. Insgesamt stellt sich die Frage, was eine gemeinsame Entscheidung beinhalten muss. Kritisch ist dabei zum einen, was den Beitrag eines individuellen gemeinsam Verantwortlichen zu dieser Entscheidung ausmacht[336] und zum anderen, welchen Auswirkungsgrad oder welche Intensität[337] dieser Beitrag erreichen muss. Wenn man annimmt, dass weder gemeinsame Zwecke noch Mittel für eine gemeinsame Entscheidung nötig wären, würde sich der Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen in der jeweiligen Billigung von Zwecken und Mittel der anderen erschöpfen. Nimmt man hingegen an, dass gemeinsame Zwecke oder gemeinsame Mittel wenigstens alternativ vorliegen müssen, wäre ein Entscheidungsbeitrag eines individuell gemeinsam Verantwortlichen zu diesen gemeinsamen Zwecken oder gemeinsamen Mitteln erforderlich. Dieser Entscheidungsbeitrag könnte auch in einem Zu-Eigen-Machen bestehen.[338]

I. Die reine Billigung von Zwecken und Mitteln als gemeinsame Entscheidung?

Bei der reinen Billigung von Zwecken und Mitteln der Verarbeitung eines fremden Akteurs drängt sich die Frage auf, inwiefern hier überhaupt ein Entscheidungsbeitrag des billigenden Akteurs vorliegt. Ausgehend von der Annahme, dass eine Billigung Divergenzen zwischen den gemeinsam Verantwortlichen hinsichtlich der Zwecke oder Mittel kompensieren soll, ist unklar, wie ein Akteur durch eine Billigung sowohl der Zwecke als auch der Mittel Einfluss oder Kontrolle auf die Verarbeitung ausüben könnte. Denn bei einer Billigung sowohl der Zwecke als auch der Mittel besteht auch kein gemeinsames Element zwischen den vermeintlich gemeinsam Verantwortlichen. Verglichen mit dem eingeschränkten Entscheidungsspielraum eines Auftragsverarbeiters wirkt ein Akteur, der nur Zwecke und Mittel billigt, noch weniger, faktisch gar nicht, auf die Verarbeitung ein. Er kann die Verarbeitung in ihrer konkreten Form durch die Billigung weder ermöglichen noch verhindern. Ob die Verarbeitung tatsächlich durchgeführt wird, ist also völlig unabhängig von der Billigung dieses Akteurs. Deutlich wird die Bedeutung der reinen Billigung von Zwecken und Mitteln bei einer der Übermitt-

[336] Dazu dieses Unterkapitel.
[337] Dazu: Kapitel 4 I. Erheblichkeitsschwelle des Entscheidungsbeitrags.
[338] Dazu: Kapitel 4 G. III. Zu-Eigen-Machen als Billigung oder Entscheidung?

lung nachgelagerten Verarbeitung durch einen empfangenden Verantwortlichen. Inwiefern der übermittelnde Verantwortliche diese nachgelagerte Verarbeitung billigt, ist nämlich völlig unerheblich.[339] Mangels einer Handlung, der die Qualität einer Entscheidung zukommt, lässt sich also bereits kein Entscheidungsbeitrag erkennen. Anhand eines Entscheidungsbeitrags auf die Verarbeitung begründet sich aber der Einfluss bzw. die Kontrolle über diese und somit die Verantwortlichkeit. Da die Billigung sowohl von Zwecken und Mitteln eines anderen Akteurs keinerlei Konsequenzen für dessen Verarbeitung hat, kann damit also auch keine gemeinsame Verantwortlichkeit begründet werden.[340]

II. Gemeinsame Zwecke oder Mittel als Identitätsgarant der Verarbeitung

Die reine Billigung fremder Zwecke und Mittel einer Verarbeitung als gemeinsame Entscheidung scheitert zudem an den wesentlichen Elementen der Mittel, jedenfalls im Verständnis der Art. 29-Datenschutzgruppe[341]. Denn die Entscheidung über die wesentlichen Elemente der Mittel betrifft die personenbezogenen Daten selbst, so etwa den Zugang, die Speicherung, vor allem aber die Auswahl der zu verarbeitenden Daten.[342] Eine Verarbeitung, die weder von denselben personenbezogenen Daten ausgeht noch verschiedene personenbezogene Daten zusammenführt,[343] entbehrt des wesentlichen Fundaments des Datenschutzrechts: Der Identität der verarbeiteten personenbezogenen Daten und damit der Identität der Verarbeitung.[344] Es liegen dann vielmehr unterschiedliche Verarbeitungen vor. Sofern nicht wenigstens die Identität der Verarbeitung gegeben ist, liegt offensichtlich kein Element vor, welches eine Gemeinsamkeit der Verarbeitung begründen könnte. Ohne gemeinsame Mittel im weiteren Sinne oder einen gemeinsamen Zweck, lässt sich aber ein Element, das einen erkennbaren Bezug zu anderen Akteuren herstellt, nicht feststellen.[345]

---

[339] Vgl. die Reichweite der gemeinsamen Verantwortung in EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 76.

[340] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung. Vgl. a. *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 47 f.

[341] Die Art. 29-Datenschutzgruppe fordert selbst entweder gemeinsame Zwecke oder Mittel: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23 ff.

[342] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[343] Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 5 Personalvermittlung.

[344] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 57: „[...] the means and purposes of the same data processing [...]".

[345] Vgl. *Bock*, K&R 2019, 30, 31 f.

Die Notwendigkeit wenigstens eines gemeinsamen Entscheidungsobjektes, also Zwecke oder Mittel, kann man begrenzt auch ErwGr 92 DSGVO entnehmen. In diesem Erwägungsgrund geht es eigentlich um die Datenschutz-Folgenabschätzung. So soll der Untersuchungsgegenstand der Datenschutz-Folgenabschätzung erweitert werden, soweit Behörden[346] oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder alternativ, wenn mehrere Verantwortliche[347] eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten. Daraus folgt die Notwendigkeit der gemeinsamen Grundlage für eine gemeinsame Verantwortlichkeit, die regelmäßig in identischen oder sich ergänzenden Mitteln bestehen wird.

Erforderlich für eine gemeinsame Entscheidung sind also immer entweder gemeinsame Zwecke oder, der in der Praxis wahrscheinlich deutlich häufigere Fall, gemeinsame Mittel im weiteren Sinne.[348] In jedem Fall ist eine Identität der Verarbeitung zu fordern. Das Szenario gemeinsamer Zwecke, aber nur gebilligter Mittel, lässt sich als Arbeitsteilung verstehen, während das Szenario gebilligter Zwecke, aber gemeinsamer Mittel gut unter den Begriff Symbiose passt.[349] Allein ein gemeinsamer Vorteil, der durch die Verarbeitung entsteht, reicht hingegen nicht aus.[350]

III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung

Zunächst lässt sich festhalten, dass die Billigung sowohl von Zwecken als auch Mitteln einer Verarbeitung nicht ausreichend für eine gemeinsame Entscheidung ist. Es müssen vielmehr wenigstens alternativ gemeinsame Zwecke oder gemeinsame Mittel, auch als Garant einer identischen Verarbeitung, vorliegen. Damit aber gemeinsame Zwecke oder gemeinsame Mittel im weiteren Sinne überhaupt vorliegen, muss ein Entscheidungsbeitrag zu einem dieser gemeinsamen Elemente vorliegen. Dieser Entscheidungsbeitrag kann, wie bereits erörtert, auch in einem Zu-Eigen-Machen

[346] Zur weiten Auslegung des Begriffs „Behörde“ durch den EuGH: EuGH, Urteil vom 09.07.2020 – C-272/19 (VQ/Hessen) = NVwZ 2020, 1497, Rn. 71, 73.

[347] Hiermit sind offensichtlich nicht öffentliche, sondern private Stellen gemeint.

[348] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23 ff. So wohl a. BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 33, der mit der gemeinsamen Verfolgung von Zwecken wohl gemeinsame Mittel meint.

[349] Vgl. zum Begriff Komplementarität Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 40.

[350] Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 40.

bestehen.[351] In jedem Fall muss ein Entscheidungsbeitrag aber Einfluss auf die Verarbeitung ausüben.

Daneben stellt sich die Frage, ob ein Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen auch hinsichtlich des divergierenden Elements, also der nicht gemeinsamen Zwecke oder Mittel, vorliegen muss. Denn unabhängig von der Notwendigkeit entweder gemeinsamer Zwecke oder gemeinsamer Mittel im weiteren Sinne muss jedenfalls eine gemeinsame Entscheidung vorliegen. Einer der neuralgischen Punkte der gemeinsamen Verantwortlichkeit ist also, ob alle gemeinsam Verantwortlichen über Zwecke **und**[352] Mittel der Verarbeitung mitentscheiden müssen.[353] Wie sich aus der Definition des singulären Verantwortlichen ergibt, setzt eine Entscheidung – als Beeinflussung der und Kontrolle über die Verarbeitung – grundsätzlich einen Entscheidungsbeitrag zu Zwecken **und** Mitteln der Verarbeitung voraus. In einem Verarbeitungsszenario mit mindestens zwei Akteuren können diese Entscheidungsbeiträge aber theoretisch zwischen den Akteuren verteilt sein. Ein gemeinsam Verantwortlicher kann also etwa über die Zwecke der Verarbeitung, ein anderer über die Mittel der Verarbeitung im Rahmen eines Entscheidungsbeitrags entscheiden. Sofern ein Entscheidungsbeitrag auch zu dem divergierenden Element, also den nicht gemeinsamen Zwecken oder Mitteln notwendig sein soll, stellt sich die Frage, was dieser beinhalten könnte. Sofern nicht durch ein Zu-Eigen-Machen des fremden Entscheidungselements bereits gemeinsame Zwecke und Mittel vorliegen, kann es sich hierbei konsequenterweise nur um eine Billigung[354] handeln.

Liegt in einem Verarbeitungsszenario mit mehreren Akteuren seitens eines Akteurs also nur ein Entscheidungsbeitrag zu den Zwecken oder Mitteln der Verarbeitung vor, stellt sich die Frage, ob damit bereits eine gemeinsame Verantwortlichkeit begründet werden kann. Mit anderen Worten stellt sich die Frage, welche Bezugspunkte der Entscheidungsbeitrag eines einzelnen gemeinsam Verantwortlichen haben muss. Falls ein Entscheidungsbeitrag nur den Zwecken oder den Mitteln nicht ausreicht, stellt sich zudem die Folgefrage, wie ein Entscheidungsbeitrag hinsichtlich divergierender Zwecke oder Mittel zu verstehen ist.

Maßgeblich für das Verständnis der gemeinsamen Entscheidung ist zudem, ob eine gemeinsame Entscheidung aufgrund einer Kumulation der Entscheidungsbeiträge verschiedener gemeinsam Verantwortlicher zu den Zwecken und Mitteln der Verarbeitung vorliegen kann. Damit stellt sich die grundlegende Frage, ob eine

[351] Dazu: Kapitel 4 G. III. Zu-Eigen-Machen als Billigung oder Entscheidung?
[352] Hervorhebung durch den Autor.
[353] *Kartheuser/Nabulsi*, MMR 2018, 717, 719.
[354] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

Arbeitsteilung hinsichtlich der gemeinsamen Entscheidung zwischen gemeinsam Verantwortlichen möglich ist. Die Alternative hierzu wäre, dass gemeinsam Verantwortliche einen einheitlichen Einigungsprozess hinsichtlich der gemeinsamen Entscheidung durchlaufen müssten.

Insgesamt lassen sich die Fragen in Bezug auf den individuellen Entscheidungsbeitrag so zusammenfassen: Über was muss entschieden werden? Wie muss entschieden werden?

1. Prozessbezogenes Verständnis der gemeinsamen Entscheidung

Ausgehend vom Wortlaut der Definition in Art. 4 Nr. 7 DSGVO („die [...] Stelle, die [...] gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet") sowie in Art. 26 Abs. 1 S. 1 DSGVO („Legen [...] Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest [...]") liegt es zunächst nahe, die gemeinsame Entscheidung so zu verstehen, dass jeder gemeinsam Verantwortliche sowohl hinsichtlich der Zwecke als auch der Mittel mitentscheiden, also einen Entscheidungsbeitrag erbringen muss.[355] Ein solch konsensuales[356] Verständnis bedeutet, dass alle gemeinsam Verantwortlichen fortwährend in alle Entscheidungen über die Verarbeitung, also jede einzelne Entscheidung über Zwecke oder Mittel, eingebunden werden.[357] Entsprechend der Beteiligung eines gemeinsam Verantwortlichen an der Entscheidung insgesamt müsste zu allen Einzelentscheidungen über die Zwecke und Mittel der Verarbeitung ein Entscheidungsbeitrag vorliegen. Eine Arbeitsteilung hinsichtlich der Entscheidung und damit der Entscheidungsbeiträge wäre nicht möglich. Ebenso wäre eine reine Kontrolle von Teilentscheidungen über Informations-, Berichts- oder Billigungserfordernisse nicht möglich. Dieses Verständnis würde die gemeinsame Entscheidung bzw. Festlegung als „miteinander vereinbaren" oder „miteinander abstimmen" auslegen.[358] Die gemeinsam Verantwortlichen müssten sich somit als Voraussetzung einer gemeinsamen Entscheidung durch einen gemeinsamen Prozess auf bestimmte Zwecke und Mittel einigen. Da in den jeweiligen Einigungsprozess

[355] *Monreal*, CR 2019, 797, Rn. 39.

[356] Vgl. *Hanloser*, ZD 2019, 455, 459.

[357] So etwa: Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 21 f.; *Kartheuser/Nabulsi*, MMR 2018, 717, 719; Gola/Heckmann/*Gola*, Art. 4 DSGVO, Rn. 67 f.; noch in der 2. Aufl.: Gola/*Piltz*, Art. 26 DSGVO, Rn. 3 ff.; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 39; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 35 f. m.w.N.; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 44; abgeschwächt: *Lezzi/Oberlin*, ZD 2018, 398, 400.

[358] *Monreal*, CR 2019, 797, Rn. 39.

immer alle gemeinsam Verantwortlichen eingebunden sein müssten, kann man aufgrund dieser (vermeintlichen) Beteiligungsnotwendigkeit von einem **prozessbezogenen**[359] **Verständnis** der gemeinsamen Entscheidung sprechen. Das Definitionselement „gemeinsam" würde also nicht nur die Entscheidung als solche, sondern auch den Entscheidungsprozess qualifizieren. Der klassische Fall einer gemeinsamen Verantwortlichkeit nach diesem prozessbezogenen Verständnis wären also zwei Akteure, die über die Verwendung einer gemeinsamen Infrastruktur oder eines gemeinsamen Datenpools in Verhandlung treten und nach der Aushandlung der Bedingungen der Verarbeitung mit dieser beginnen.

Neben dieser strengen Variante des prozessbezogenen Verständnisses wäre noch eine weichere Variante denkbar, die einen einzelnen Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen zu den Zwecken als auch den Mitteln der Verarbeitung erfordert. Diese weiche Variante scheint aber zu willkürlich in ihren Voraussetzungen um einen systematischen Mehrwert zu bieten. Der einzige Vorteil dieser weichen Variante würde darin liegen, dass triviale Entscheidungen im Bereich der Mittel, also solche über die unwesentlichen Elemente der Mittel, hinsichtlich des Entscheidungsprozesses ausgeblendet werden könnten.

Konsequenz des prozessbezogenen Verständnisses wäre, dass wenn ein Verantwortlicher an einer bestimmten Entscheidung über Zwecke oder Mittel nicht durch einen eigenen Entscheidungsbeitrag beteiligt wäre, er nicht gemeinsam Verantwortlicher würde. Eine gemeinsame Entscheidung nach dem prozessbezogenen Verständnis wäre also stark formalisiert. Nicht mit dem prozessbezogenen Verständnis vereinbar wären zudem Entscheidungsbeiträge, die in Unkenntnis des Gesamtbildes der Verarbeitung erfolgen würden. Also etwa, wenn einem Akteur nicht bekannt ist, dass ein anderer an der Verarbeitung beteiligter Akteur nachträglich weitere Akteure einbindet. Ebenso wäre es mit dem prozessbezogenen Verständnis unvereinbar, wenn einem Akteur die Identität anderer an der Verarbeitung Beteiligter zum Zeitpunkt seines Entscheidungsbeitrags unbekannt wäre. Denn in diesem Fall wäre der Entscheidungsprozess des einen Akteurs bereits abgeschlossen, bevor der andere Akteur an diesem Prozess beteiligt werden könnte. Hiermit unvereinbar wäre etwa der Sachverhalt in der Rechtssache Fashion ID.[360] Dort fand ein Einigungsprozess des Websitebetreibers mit dem Plattformbetreiber vor Einbindung des Social Plugin gerade nicht statt. Es handelte sich vielmehr um ein „take-it-or-leave-it"-Angebot.

[359] In Abgrenzung zum Begriff des Verarbeitungsvorgangs oder -prozesses könnte man hier a. von einem verfahrensbezogenen Verständnis sprechen.

[360] Dazu: Kapitel 4 B. III. Fashion ID.

Hinsichtlich des „was“ der gemeinsamen Entscheidung lässt sich für das prozessbezogene Verständnis also festhalten, dass sowohl über Zwecke als auch Mittel der Verarbeitung durch einen individuellen Verantwortlichen entschieden werden muss. Hinsichtlich des „wie“ lässt sich festhalten, dass ein gemeinsamer Entscheidungsprozess notwendig ist.

2. Ergebnisbezogenes Verständnis der gemeinsamen Entscheidung

Allerdings lässt sich der Wortlaut der Definition der gemeinsam Verantwortlichen auch so verstehen, dass die gemeinsam Verantwortlichen nur als Ergebnis ihrer Zusammenarbeit über die Zwecke und Mittel der Verarbeitung entschieden haben müssen.[361] Demnach könnte etwa ein gemeinsam Verantwortlicher über die Zwecke entscheiden, ein anderer gemeinsam Verantwortlicher über die Mittel. Je nach Anzahl der beteiligten Akteure könnten die Einzelentscheidungen, insbesondere über die Mittel, noch weiter zwischen den gemeinsam Verantwortlichen aufgeteilt sein. Erforderlich für die gemeinsame Verantwortlichkeit eines individuellen Verantwortlichen wäre demnach nur ein Entscheidungsbeitrag zu einem der beiden Entscheidungsobjekte, also zu den Zwecken oder zu den Mitteln. Denkbar wäre nach diesem Verständnis auch eine Arbeitsteilung hinsichtlich der Entscheidung, es müssten nicht zwangsläufig immer alle Akteure in jede Teilentscheidung eingebunden werden.[362] Nach diesem Verständnis wäre zudem eine zeitliche Trennung der verschiedenen Entscheidungen und auch eine fehlende Kenntnis der anderen gemeinsam Verantwortlichen unschädlich. Denn für die gemeinsame Entscheidung käme es nur auf die Kumulation der Entscheidungsbeiträge an.

Soweit nach diesem Verständnis allerdings Entscheidungsbeiträge verschiedener Akteure vorliegen und kein spezifischer Einigungsprozess vorausgesetzt wird, ist ein Mechanismus notwendig, der garantiert, dass den jeweiligen Akteuren nicht

---

[361] So etwa: *Brühann*, 2.4 Europarechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 21. Scheinbar a.: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22: „[...] schließt die Möglichkeit, dass verschiedene Akteure an verschiedenen Vorgängen oder Vorgangsreihen im Zusammenhang mit personenbezogenen Daten beteiligt sind, nicht aus. Diese Vorgänge können gleichzeitig oder in verschiedenen Stadien durchgeführt werden.“

[362] Sydow/Marsch/*Ingold*, Art. 26 DSGVO, Rn. 1, 4; *Lachenmann*, Datenübermittlung im Konzern, 2016, 63; wohl a.: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 46 ff.; Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 8 f.; *Jung/Hansch*, ZD 2019, 143, 144, 147. Unklar in Bezug auf unbewusste Entscheidungen (Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 12) bleibt: Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DS-GVO, Rn. 13. Ebenso unklar: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 52.

Entscheidungsbeiträge gegen ihren Willen aufgezwungen werden. Es muss sich also im Ergebnis um eine gemeinsame Entscheidung, getragen von allen beteiligten Akteuren, handeln. Denkbar ist in solchen arbeitsteiligen Prozessen grundsätzlich, auf Abstimmungs- oder Berichtspflichten abzustellen.[363] Allerdings sind auch Szenarien denkbar, in denen Verantwortliche hierauf verzichten oder dies schlicht faktisch nicht möglich ist. Dies gilt etwa für massenhafte Angebote oder die Bereitstellung von Infrastruktur. Ein Element, das die Entscheidungsbeiträge der anderen gemeinsam Verantwortlichen zu einer gemeinsamen Entscheidung verbindet, könnte zunächst in dem Zu-Eigen-Machen gesehen werden. Allerdings hat das Zu-Eigen-Machen, wie bereits erörtert, selbst den Charakter eines Entscheidungsbeitrags.[364] Denkbar ist zwar, dass sowohl ein eigener Entscheidungsbeitrag zu dem einen Entscheidungsobjekt als auch ein Zu-Eigen-Machen eines Entscheidungsbeitrags zu dem anderen Entscheidungsobjekt seitens eines individuellen Verantwortlichen vorliegt. Allerdings ist es ebenso denkbar, dass gar kein eigener Entscheidungsbeitrag besteht, sondern nur das Zu-Eigen-Machen eines fremden Entscheidungsbeitrags. In diesem Fall lägen immer noch andere fremde Entscheidungsbeiträge, etwa zu den Zwecken oder Mitteln vor, die zu einer gemeinsamen Entscheidung verbunden werden müssten. Ein solch verbindendes Element kann in der Billigung fremder Entscheidungsbeiträge gesehen werden.[365] Diese Billigung ist dann zwar als notwendiger Teil der gemeinsamen Entscheidung zu werten, allerdings nicht selbst als ein Entscheidungsbeitrag zu den Zwecken oder Mitteln der Verarbeitung. Denn es wäre nicht klar, wie sich die Billigung als vermeintlicher Entscheidungsbeitrag auf ein divergierendes Entscheidungsobjekt auswirken sollte.

Da es bei diesem Verständnis der gemeinsamen Entscheidung nur darauf ankommt, dass in der Summe der Zusammenarbeit eine Entscheidung über die Zwecke und Mittel der Verarbeitung vorliegt, kann man hierbei von einem **ergebnisbezogenen**[366] **Verständnis** der gemeinsamen Entscheidung sprechen. Auch eine Entscheidung nach dem prozessbezogenen Verständnis wäre im Rahmen des ergebnisbezogenen Verständnisses eine gemeinsame Entscheidung. Denn der maßgebliche Unterschied

[363] Noch in der 3. Aufl.: Plath/*Plath*, Art. 26 DSGVO, Rn. 8. Missverständlich: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 41.

[364] Dazu: Kapitel 4 G. III. Zu-Eigen-Machen als Billigung oder Entscheidung?

[365] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

[366] Vergleiche a. die Darstellung von gemeinsam Verantwortlichen als „jointly" oder „in common" bei Kuner/Bygrave/Docksey/*Millard/Kamarinou*, Art. 26 GDPR, 584 und *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 31 Fn. 75. „Jointly" bedeutet dabei ein gemeinsames Handeln der Akteure, während „in common" einen Informationspool vorsieht, in dem Informationen unabhängig von Akteuren untereinander verarbeitet werden.

zwischen dem ergebnisbezogenen und prozessbezogenen Verständnis der gemeinsamen Entscheidung ist, dass das ergebnisbezogene Verständnis keinen spezifischen Einigungsprozess voraussetzt, sondern diesen Prozess durch das Element der (impliziten) Billigung kompensiert. Innerhalb der Entscheidungsaufteilung zwischen gemeinsam Verantwortlichen wäre ebenso ein Entscheiden miteinander möglich. Im ergebnisbezogenen Verständnis wird vor allem der Kontrollaspekt der Verantwortlichkeit betont.[367] Insgesamt müssten gemeinsam Verantwortliche aber über alle notwendigen Aspekte der Zwecke und Mittel der Verarbeitung schlussendlich entschieden haben.[368] Ein klassischer Fall für das ergebnisbezogene Verständnis lässt sich kaum bilden, da das extensive Verständnis eine Unzahl von Verarbeitungsszenarien erfassen würde. In jedem Fall sind die Sachverhalte aus den Entscheidungen des EuGH zu den gemeinsam Verantwortlichen beispielhaft für das ergebnisbezogene Verständnis der gemeinsamen Entscheidung.[369]

Hinsichtlich des „was" der gemeinsamen Entscheidung lässt sich für das ergebnisbezogene Verständnis also festhalten, dass entweder über Zwecke oder Mittel der Verarbeitung durch einen individuellen Verantwortlichen entschieden werden muss. Hinsichtlich des „wie" lässt sich festhalten, dass divergierende Entscheidungsbeiträge anderer gemeinsam Verantwortlicher gebilligt werden müssen.

Die gemeinsame Entscheidung lässt sich also zum einen prozessbezogen verstehen, zum anderen ergebnisbezogen. Man kann das prozessbezogene Verständnis auch als enges Verständnis der gemeinsamen Entscheidung verstehen, während das ergebnisbezogene Verständnis ein weites Verständnis darstellt. Im Hinblick auf den Wortlaut vertretbar scheinen zunächst beide Interpretationen.[370]

3. Das Verständnis der gemeinsamen Entscheidung nach dem Wortlaut der DSGVO

a) Art. 4 Nr. 7 DSGVO

Zunächst ließe sich einwenden, das prozessbezogene Verständnis der gemeinsamen Entscheidung wäre ausgehend vom Wortlaut der Definition in Art. 4 Nr. 7 DSGVO naheliegender. Denn der Unionsgesetzgeber hätte spätestens im Rahmen der DSGVO

[367] Siehe etwa: *Hacker*, MMR 2018, 779, 780.
[368] *Alsenoy*, CLSR[28] (2012), 25, 31.
[369] Dazu: Kapitel 4 H. III. 5. Das Verständnis der gemeinsamen Entscheidung in der Rechtsprechung des EuGH.
[370] Dies übersehen *Kartheuser/Nabulsi*, MMR 2018, 717, 720. Insofern sind a. nicht systematische oder teleologische Gründe für eine diesbezügliche Auslegung erforderlich.

entweder ein „oder“ in die Definition einfügen können[371] oder die Definition um den minimalen Entscheidungsbeitrag eines gemeinsam Verantwortlichen erweitern können, falls er die gemeinsame Entscheidung ergebnisbezogen versteht. Feststellen lässt sich allerdings, dass der Unionsgesetzgeber trotz der Ausführungen der Art. 29-Datenschutzgruppe in WP 169[372] keinerlei Änderungen der Definition gegenüber der DSRL vorgenommen hat. Es bestand also anscheinend kein Präzisierungsbedarf hinsichtlich der Definition.[373] Ob die Erweiterung der Definition um ein „oder“ den gewünschten Erfolg gebracht hätte, lässt sich bezweifeln. Die Paralleldefinition des singulären Verantwortlichen in Art. 4 Nr. 7 DSGVO bedingt, dass in jedem Fall insgesamt eine Entscheidung über Zwecke und Mittel der Verarbeitung vorliegen muss. Andernfalls wird eine Verantwortlichkeit schlicht nicht begründet.[374] Eine Umformulierung der Definition wie etwa: „die [...] Stelle, die allein oder gemeinsam mit anderen über die Zwecke **und/oder** Mittel [...] entscheidet“, hätte für den singulären Verantwortlichen keinen Sinn ergeben. Sie hätte bestenfalls die Definition weiter verkompliziert und damit sowohl unverständlicher gemacht als auch für weitere Auslegungen geöffnet. Die Paralleldefinition des singulären Verantwortlichen ist offensichtlich nur ergebnisbezogen zu verstehen, da sie keine weiteren Akteure berücksichtigen muss. Somit gibt es auch keine Ansatzpunkte, vor allem aber auch keine Erforderlichkeit für einen bestimmten Entscheidungsprozess bei der Definition des singulären Verantwortlichen.

b) Art. 26 Abs. 1 S. 1 DSGVO

Nur bei gemeinsam Verantwortlichen stellt sich überhaupt die Frage, ob die gemeinsame Entscheidung prozessbezogen oder ergebnisbezogen zu verstehen ist. Art. 26 Abs. 1 S. 1 DSGVO, der entgegen Art. 4 Nr. 7 DSGVO nur die gemeinsam Verantwortlichen definiert, ist in dieser Hinsicht aber auch nicht eindeutiger. So gibt Art. 26 Abs. 1 S. 1 DSGVO weder den individuellen Entscheidungsbeitrag eines gemeinsam Verantwortlichen vor noch die notwendigen Entscheidungsobjekte, also Zwecke und/oder Mittel eines solchen Entscheidungsbeitrags. Gemeinsam

[371] Also „ [...] über die Zwecke **oder** Mittel der Verarbeitung von personenbezogenen Daten entscheidet;“

[372] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 21 ff.

[373] Angemerkt sei hier, dass EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357 erst seit Anfang 2016 als Vorlage am EuGH anhängig war, somit also im Gesetzgebungsprozess der DSGVO keine Rolle mehr spielen konnte.

[374] Ähnlich noch in der. 3. Aufl.: Plath/*Plath*, Art. 26 DSGVO, Rn. 9.

Verantwortliche müssen nach dem Wortlaut von Art. 26 Abs. 1 S. 1 DSGVO nur gemeinsam Zwecke und Mittel der Verarbeitung festlegen. Ob das „gemeinsam" sich dabei auf den Prozess oder das Ergebnis der Festlegung bezieht, wird nicht deutlich, da nur die Gesamtheit der gemeinsam Verantwortlichen von Art. 26 Abs. 1 S. 1 DSGVO erfasst wird. Die Möglichkeit individueller Entscheidungsbeiträge eines gemeinsam Verantwortlichen oder Varianten einer gemeinsamen Verantwortlichkeit zeigt die Definition also nicht auf.

Festhalten lässt sich, dass der Wortlaut der Definitionen in Art. 4 Nr. 7 und Art. 26 Abs. 1 S. 1 DSGVO jedenfalls ein ergebnisbezogenes Verständnis dergestalt nicht ausschließt, nach dem ein individueller gemeinsam Verantwortlicher alternativ nur zu den Zwecken oder Mitteln der Verarbeitung einen Entscheidungsbeitrags leistet und andere Entscheidungsbeiträge, etwa hinsichtlich des anderen Entscheidungsobjektes, billigt.

4. Das Verständnis der gemeinsamen Entscheidung nach Auffassung der Aufsichtsbehörden

a) Art. 29-Datenschutzgruppe

Im WP 169, welches deutlich vor der Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit veröffentlicht wurde, hatte die Art. 29-Datenschutzgruppe die Auffassung vertreten, dass eine gemeinsame Kontrolle[375] dann gegeben sei, wenn verschiedene Parteien im Zusammenhang mit spezifischen Verarbeitungen entweder über den Zweck oder über die wesentlichen Elemente der Mittel entscheiden.[376] Die Entscheidung über die Zwecke der Verarbeitung führe zwangsläufig zu einer Einstufung als Verantwortlicher, die Entscheidung über die wesentlichen Elemente der Mittel impliziere sie hingegen nur.[377] Dabei sei der Fall, dass mehrere Akteure über alle Zwecke und Mittel der Verarbeitungstätigkeiten gemeinsam entscheiden, indem sie gemeinsame Mittel für die Erreichung gemeinsamer Zwecke einsetzen, ein eindeutiger und unproblematischer Fall einer gemeinsamen Verantwortlichkeit, allerdings nicht

[375] Im Sinne einer gemeinsamen Entscheidung.

[376] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23.

[377] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17. Diese Ausführungen finden sich zwar in den allgemeinen Ausführungen zu Zwecken und Mitteln der Verarbeitung, machen allerdings nur im Hinblick auf gemeinsam Verantwortliche Sinn.

der einzige.[378] Die gemeinsame Verantwortlichkeit könne verschiedene Formen aufweisen, von völlig übereinstimmenden Zwecken und Mitteln über die Übereinstimmung nur von Zwecken oder Mitteln oder auch nur Teilen davon.[379] Dabei könne die Beteiligung gemeinsam Verantwortlicher an Verarbeitungsvorgängen gleichzeitig oder in verschiedenen Stadien erfolgen.[380] Grundsätzlich solle bei gemeinsam Verantwortlichen die Bestimmung der Verantwortlichkeit spiegelbildlich zu singulären Verantwortlichen erfolgen.[381]

b) Europäischer Datenschutzbeauftragter (EDPS)

Der EDPS scheint sich dieser Auffassung anzuschließen.[382] So seien die Zwecke und Mittel der Verarbeitung zwar miteinander verbunden, allerdings könne der Grad des Einflusses auf diese beiden Objekte zwischen gemeinsam Verantwortlichen variieren.[383] Insgesamt müsse aber über Zwecke und Mittel der Verarbeitung entschieden worden sein. Die Erwähnung der Varianz des möglichen Einflusses könnte darauf hindeuten, dass die Billigung eines fremden Entscheidungsbeitrags zu einem Entscheidungsobjekt ausreicht, sofern ein eigener Entscheidungsbeitrag zu dem anderen vorliegt. Die Frage, ob der Entscheidungsprozess selbst gemeinsam, also mit Beteiligung aller Akteure, durchgeführt werden muss, thematisieren die Guidelines nicht.[384]

---

[378] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22, 26.

[379] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23 f. Eine Typologie entwickelt die Art. 29-Datenschutzgruppe dabei nicht: *Alsenoy*, CLSR[28] (2012), 25, 32. Überblicksartig zu den Beispielen in WP 169: *Söbbing*, ITRB 2020, 218, 219.

[380] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[381] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[382] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9 f. S. 23 f. erscheint hingegen etwas widersprüchlicher, da der EDPS anscheinend bereits durch die Billigung und das Eingehen einer Vereinbarung eine gemeinsame Verantwortlichkeit annimmt. Dies könnte wiederum als ein sich Zu-Eigen-Machen verstanden werden. Insgesamt wirken die Guidelines etwas unfertig. Deutlich wird dies an der unsystematischen Wiedergabe der jüngeren EuGH-Rechtsprechung auf S. 10 a.E.

[383] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9.

[384] Vgl. „entering into such agreement“: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 23.

c) Europäischer Datenschutzausschuss (EDPB)

Neben der Möglichkeit einer gemeinsamen Entscheidung („common decision") sieht der EDPB die Möglichkeit einer „converging decision" – im Deutschen wohl am ehesten mit konvergierender oder zusammenfließender Entscheidung zu übersetzen – vor.[385] Die „converging decision" wird insoweit zur gemeinsamen Entscheidung abgegrenzt, als dass die gemeinsame Entscheidung ein Entscheiden zusammen und eine geteilte Absicht voraussetze.[386] Gemeint ist damit wohl ein gemeinsamer Entscheidungsprozess. Die Möglichkeit einer „converging decision" soll sich vor allem aus den Urteilen des EuGH ergeben.[387] Entscheidungen sollen dann als konvergierend im Hinblick auf Zwecke und Mittel angesehen werden, wenn sie sich wechselseitig ergänzen und für eine Verarbeitung dergestalt notwendig sind, dass sie einen spürbaren Einfluss auf die Entscheidung über die Zwecke und Mittel der Verarbeitung haben. Demnach soll ein wichtiges Kriterium für die Bestimmung einer „converging decision" sein, ob eine Verarbeitung ohne die Beteiligung beider Parteien hinsichtlich der Zwecke und Mittel stattgefunden hätte, also die Verarbeitung seitens jeder Partei untrennbar miteinander verbunden ist.[388] Dabei soll die „converging decision" aber nur im Hinblick auf die Zwecke und Mittel der Verarbeitung verstanden werden und gerade nicht im Hinblick auf andere Aspekte einer kommerziellen Beziehung zwischen den Parteien.[389] Diese wechselseitige Ergänzung kann als die bereits erwähnte Zweckkomplementarität verstanden werden.[390]

Während die Art. 29-Datenschutzgruppe, wie bereits dargestellt, davon ausging, dass sowohl die isolierte Entscheidung[391] über die Zwecke als auch die isolierte Entscheidung über die (wesentlichen Elemente der) Mittel ausreichend für eine

[385] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 54.

[386] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

[387] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

[388] Die Wortwahl des EDPB in *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 54, 55 ist dabei verwirrend. So ist zunächst die Rede von „two or more entities" bei einer „converging decision", dann aber später nur von „each other" und „both parties". Wie genau diese „converging decision" bei mehr als zwei Beteiligten funktioniert, wäre aber durchaus ausführungsbedürftig.

[389] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 55.

[390] Dazu: Kapitel 4 E. I. 6. „Interesse" als Zweckkomplementarität.

[391] Gemeint ist damit wohl der Entscheidungsbeitrag.

gemeinsame Verantwortlichkeit ist,[392] finden sich in der Rechtsprechung des EuGH bislang keine deutlichen Ausführungen, die diese Ansicht unterstützen.[393] Da der EuGH dieses Verständnis also offenbar nicht aufgegriffen hat, dürfte der EDPB als Nachfolgergremium der Art. 29-Datenschutzgruppe seine eigene Auffassung wiederum an die Rechtsprechung des EuGH im Rahmen der „converging decisions" angepasst haben.[394] Andererseits kann man die „converging decisions" als einerseits die Billigung divergierender Entscheidungsbeiträge[395] sowie andererseits sich ergänzende Entscheidungsbeiträge verstehen. Hinsichtlich der untrennbaren Verbindung der beteiligten Parteien durch die Verarbeitung ist es denkbar, dass der EDPB auf die Rechtsprechung des EuGH zum Anwendungsbereich der Niederlassung Bezug nimmt.[396] Dort hatte der EuGH auf eine untrennbare Verbindung der Werbegeschäftstätigkeit einer Niederlassung mit dem Betrieb einer Suchmaschine durch den Verantwortlichen erkannt.

Der EDPB illustriert die „converging decisions" mit dem Beispiel einer Personalvermittlung.[397] In diesem Beispiel hilft Unternehmen X dem Unternehmen Y bei der Rekrutierung neuer Mitarbeiter im Rahmen eines Mehrwertdienstes. Unternehmen X sucht dabei nach potenziellen Mitarbeitern in den Lebensläufen, die bei Unternehmen Y ankommen, sowie in seiner eigenen Datenbank. Diese Datenbank wurde von X allein erstellt und wird ebenso von ihm allein betrieben. X erhöht mit der Datenbank seine Vermittlungschancen und somit seinen Umsatz. Auch ohne eine formelle Entscheidung sollen X und Y gemeinsam an dieser Verarbeitung mit dem Zweck der Suche nach geeigneten Kandidaten aufgrund von „converging decisions" beteiligt sein. Diese „decisions" sollen zum einen die Entscheidung von X sein, die eigene Datenbank zu betreiben und zum anderen die Entscheidung von Y sein, diese Datenbank mit den selbst erhaltenen Lebensläufen anzureichern. Diese Entscheidungen sollen komplementär, untrennbar und notwendig für die

[392] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23.

[393] Insofern erscheint die Kritik an der unklaren Rechtsprechung bei *Kartheuser/Nabulsi*, MMR 2018, 717, 720 berechtigt.

[394] In *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 36 wird nicht klar, ob dies allein das Verhältnis zum Auftragsverarbeiter betrifft.

[395] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

[396] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 47, 56.

[397] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 5 Personalvermittlung. Dieses Beispiel wiederum basiert offensichtlich auf *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23 Beispiel 6.

Verarbeitung sein, um geeignete Kandidaten zu finden. Folglich bestehe eine gemeinsame Verantwortlichkeit. Allerdings sei X singulärer Verantwortlicher für die Verarbeitungen, die zum Betrieb der Datenbank notwendig seien und Y singulärer Verantwortlicher für die nachfolgenden Verarbeitungen im Rahmen der Einstellung. Die gemeinsame Verantwortlichkeit bestehe also nur für die Verarbeitungsvorgänge, die notwendig sind, um eine Liste potenzieller Mitarbeiter zu generieren.

Daneben weist der EDPB darauf hin, dass die Analyse der gemeinsamen Verantwortlichkeit eine Analyse von Fall zu Fall und Vorgang zu Vorgang erfordere.[398] Nicht jede Beteiligung verschiedener Akteure an einer Verarbeitung stelle automatisch eine gemeinsame Verantwortlichkeit dar. Dies versucht der EDPB mit mehreren Beispielen zu illustrieren. All diesen ist gemein, dass – nach dem Verständnis des EDPB – keine gemeinsame Entscheidung über Zwecke und Mittel vorliegt. Unter anderem stelle die reine Übermittlung zwischen Verantwortlichen, etwa im Rahmen der Übermittlung von Arbeitnehmerdaten an eine Steuerbehörde, keine gemeinsame Verantwortlichkeit dar.[399] Gleiches gelte für die Übermittlung personenbezogener Daten seitens eines Reisebüros an ein Hotel oder eine Airline zwecks Reservierung für ein Reisepaket.[400] Es fehle ebenso an einer gemeinsamen Verantwortlichkeit, wenn zwar eine geteilte Datenbank oder eine gemeinsame Infrastruktur genutzt werde, allerdings die Zwecke unabhängig voneinander festgelegt werden.[401] Dies gelte etwa im Hinblick auf eine konzerninterne oder externe Auftragsverarbeitung. Zudem liege auch dann keine gemeinsame Verantwortlichkeit vor, wenn verschiedene Akteure dieselben personenbezogene Daten zwar in einer Kette von Verarbeitungen verarbeiten würden, dabei allerdings unabhängig voneinander über die Zwecke und Mittel der Verarbeitung entscheiden.[402] Dies sei etwa dann der Fall, wenn eine öffentliche Stelle zu einem bestimmten Thema Analysen und Statistiken erarbeite und dafür von anderen

[398] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 69.

[399] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 70 Beispiel; vorher bereits die Art. 29-Datenschutzgruppe: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 25 Beispiel 9.

[400] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 68 Beispiel 1 Reisebüro; vorher bereits die Art. 29-Datenschutzgruppe: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24 Beispiel 7 (Reisebüro (1)).

[401] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 71. Gegenbeispiel: ebd., Rn. 68 Beispiel 6 Analyse von Gesundheitsdaten.

[402] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 72.

öffentlichen Stellen Daten anfordere. Insgesamt grenzt der EDPB also die gemeinsame Verantwortlichkeit von der reinen Übermittlung zwischen Akteuren sowie der Auftragsverarbeitung ab.

5. Das Verständnis der gemeinsamen Entscheidung in der Rechtsprechung des EuGH

Bis zu dem Urteil in der Rechtssache NZÖG[403] war eine explizite Stellungnahme des EuGH zu dem Verständnis der gemeinsamen Entscheidung nicht auszumachen. Aber auch nach diesem Urteil dürfte der EuGH noch weitere Vorlageverfahren im Kontext der gemeinsamen Entscheidung entscheiden müssen. Die folgenden Ausführungen stellen die Urteile des EuGH daher im Kontext der gemeinsamen Entscheidung dar und ordnen sie ein.

a) Google Spain

In dem Urteil zu der Rechtssache Google Spain[404] erwähnte der EuGH in den Rn. 38 und 40 zwar hinsichtlich der Entscheidung des Verantwortlichen[405] insgesamt die Zwecke und Mittel der Verarbeitung. Er ließ es in Rn. 40, in einer Art Reserveerwägung für die Verantwortlichkeit des Suchmaschinenbetreibers, allerdings für eine gemeinsame Verantwortlichkeit zwischen dem Suchmaschinenbetreiber und dem Herausgeber einer Website genügen, dass Suchmaschinenbetreiber und Websiteherausgeber[406] gemeinsam über die Mittel der Verarbeitung der Suchmaschine anhand der robot.txt-Datei entscheiden.[407] Nur weil der Herausgeber einer Website anhand einer robot.txt-Datei seine Website indexieren oder nicht indexieren lassen wolle, entbinde dies den Suchmaschinenbetreiber nicht von seiner eigenen Verantwortung. Anscheinend soll aufgrund dieser gemeinsamen Entscheidung über die Mittel, im Rahmen der robot.txt-Datei, also eine gemeinsame Verantwortlichkeit denkbar sein. Diese konnte sich dann allerdings nur auf die Verarbeitungen der personenbezogenen Daten auf der indexierten Website des Herausgebers beziehen. Die Ausführungen des EuGH zur gemeinsamen Verantwortlichkeit in der Rechtssache Google Spain sind insgesamt äußerst knapp. In seiner späteren Rechtsprechung zur

[403] Dazu unten.
[404] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857.
[405] In diesem Fall eines Suchmaschinenbetreibers.
[406] Diesen Begriff verwendet das Urteil.
[407] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 40; siehe a.: Kuner/Bygrave/Docksey/*Millard/Kamarinou*, Art. 26 GDPR, 584 f.

gemeinsamen Verantwortlichkeit nahm der EuGH auf diese Ausführungen auch nicht weiter Bezug.

b) Jehovan todistajat

Das Urteil zu der Rechtssache Jehovan todistajat[408] stützt weder das prozessbezogene Verständnis noch das ergebnisbezogene Verständnis der gemeinsamen Entscheidung notwendigerweise, da zwischen der Religionsgemeinschaft und ihren verkündenden Mitgliedern jedenfalls der gemeinsame Zweck bestand, den Glauben dieser Gemeinschaft zu verbreiten.[409] Die Entscheidung über die Zwecke der Verarbeitung zieht – etwa auch nach Ansicht der Art. 29-Datenschutzgruppe – eine unbedingte Einordnung als gemeinsamer Verantwortlicher nach sich.[410] Daneben konnten zwar gewisse Ausführungen des EuGH zur Koordination der Verkündigungstätigkeit durch die Glaubensgemeinschaft als Entscheidungsbeitrag zu den Mitteln verstanden werden.[411] Mangels hinreichender Sachverhaltsangaben in der Vorlage sind diese Ausführungen allerdings nur begrenzt belastbar.

c) Wirtschaftsakademie

In dem Urteil zu der Rechtssache Wirtschaftsakademie[412] wurde ebenso nicht deutlich, ob individuelle Entscheidungsbeiträge der gemeinsam Verantwortlichen bezüglich der Zwecke (prozessbezogenes Verständnis) oder nur jeweils eigene Zwecke sowie eine Billigung der jeweils fremden Zwecke (ergebnisbezogenes Verständnis) vorlagen. Gemeinsame Mittel waren im Hinblick auf die Fanpage hingegen eindeutig gegeben. Denn durch die Einrichtung der Fanpage machte sich der Fanpage-Betreiber dieses Mittel, im technischen Sinne, zu eigen. Problematisch erweist sich bei einer Analyse der Rechtssache Wirtschaftsakademie insbesondere, dass der EuGH nicht unmittelbar unter die einzelnen Elemente der Definition des gemeinsam Verantwortlichen subsumierte.

---

[408] Dazu: Kapitel 4 B. II. Jehovan todistajat.

[409] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 44, 71.

[410] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17. Vgl. a. das Szenario BYOD bei *Jung/Hansch*, ZD 2019, 143, 146.

[411] Kritisch zur fehlenden Differenzierung zwischen Zwecken und Mitteln: *Jung/Hansch*, ZD 2019, 143, 144.

[412] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

In Rn. 36 erfolgte eine Subsumtion dahingehend, dass ein Beitrag des Fanpage-Betreibers zur Verarbeitung vorliege.[413] Dieser Beitrag scheint sich aus der Einrichtung und Parametrierung der Fanpage zu ergeben. In Rn. 39 wiederum wurde die Beteiligung des Fanpage-Betreibers an der gemeinsamen Entscheidung über Zwecke und Mittel festgestellt.[414] Die vorhergehenden Ausführungen in Rn. 34[415] dürften dabei die Zwecke der Verarbeitung beschreiben. Hier stellte der EuGH die Zwecke getrennt für den Plattformbetreiber und den Fanpage-Betreiber dar. Für Facebook sei der Zweck die Verbesserung seines Werbesystems, für den Fanpage-Betreiber die Verbesserung seines Marketings anhand der Statistik. Im Gegensatz zu dem späteren Urteil in der Rechtssache Fashion ID wurde kein verbindendes Element eines wirtschaftlichen Interesses durch den EuGH festgestellt.[416] Folglich liegt es fern, dass der EuGH mit diesen Ausführungen einen gemeinsamen Entscheidungsprozess, im Sinne des prozessbezogenen Verständnisses, der gemeinsamen Entscheidung darstellen wollte.[417] Man kann diesen Ausführungen stattdessen vielmehr entnehmen, dass der Zweck des jeweils anderen gemeinsam Verantwortlichen gebilligt wird. Dies gilt insbesondere im Hinblick auf die bloße Beteiligung an der Entscheidung über Zwecke und Mittel nach Rn. 39. Dort heißt es: „ [...] dass der [Fanpage-]Betreiber [...] an der Entscheidung über die Zwecke und Mittel der Verarbeitung [...] beteiligt ist." Denkbar ist also ein Entscheidungsbeitrag des Fanpage-Betreibers bezüglich der Mittel und eine „Beteiligung", etwa im Sinne einer Billigung, bezüglich der Zwecke. Dies würde auf ein ergebnisbezogenes Verständnis der gemeinsamen Entscheidung hindeuten.

Als Nachweis für die Billigung fremder Zwecke statt eines gemeinsamen Entscheidungsprozesses kann auch Rn. 36 verstanden werden.[418] Dort führte der EuGH aus, dass die Einrichtung einer Fanpage eine Parametrierung dieser und damit eine Auswirkung auf die Erstellung der Besucherstatistiken impliziere. Dies stelle einen Beitrag zur Verarbeitung der Besucherdaten dar. Aufgrund der durch den Plattformbetreiber vorgegebenen Parametrierungsmöglichkeiten hinsichtlich von „Zielen der Steuerung oder Förderung seiner [des Fanpage-Betreibers] Tätigkeiten" kann man eine vorgelagerte Billigung eben dieser Ziele des Fanpage-Betreibers, also seiner Zwecke, durch den Plattformbetreiber annehmen.[419] Dem Fanpage-Betreiber

[413] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36.
[414] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 39.
[415] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34.
[416] Dazu: Kapitel 4 E. I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen.
[417] So versteht wohl a. *Hacker*, MMR 2018, 779, 780 die Ausführungen des EuGH.
[418] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36.
[419] Kritisch zur Antizipation: *Moos/Rothkegel*, MMR 2019, 584, 585 f.

wiederum sind die Zwecke des Plattformbetreibers jedenfalls zum Zeitpunkt der Einrichtung der Fanpage bekannt.

Geht man andererseits davon aus, dass die durch den Plattformbetreiber vorgegebenen Parametrierungsmöglichkeiten hinsichtlich von „Zielen der Steuerung oder Förderung seiner [des Fanpage-Betreibers] Tätigkeiten" einen Entscheidungsbeitrag des Plattformbetreibers im Hinblick auf gemeinsame Zwecke darstellen, also nicht nur eine Billigung, ist dies kaum zielführend. Denn zum einen besteht offensichtlich kein gemeinsamer Zweck des Fanpage-Betreibers und Plattformbetreibers. Es wäre also unklar, worin der Entscheidungsbeitrag des Plattformbetreibers bestehen sollte, sofern mit der Vornahme der Parametrierung nur ein eigener Zweck des Fanpage-Betreibers bekundet wird.[420] Zum anderen stellte der spezifische Sachverhalt, unterstellt bei der Parametrierung der Fanpage handelt es sich überhaupt um einen Entscheidungsbeitrag hinsichtlich der Zwecke, auch einen klaren Sonderfall dar.[421]

Deutlich widerspruchsfreier und unkomplizierter ist es daher, die Parametrierung des Zielpublikums, neben der generellen Ermöglichung der Verarbeitung durch den Fanpage-Betreiber, als dessen Entscheidungsbeitrag zu den Mitteln zu erachten.[422] Da es bei der Parametrierung des Zielpublikums um die Frage geht, welche Daten überhaupt für die Statistik verarbeitet werden sollen, sind zudem die wesentlichen Elemente[423] der Mittel betroffen. Auswirkungen hat diese Parametrierung nur auf die der Erhebung der Daten folgende Verarbeitung zu den vom Plattformbetreiber erstellten Statistiken.[424] Zwar ist die vorherige Erhebung von Daten durch den Plattformbetreiber offensichtlich notwendig für die Erstellung der Statistiken, allerdings beeinflusst der Fanpage-Betreiber diese Erhebung eigentlich nur dahingehend, dass er sie durch die Eröffnung der Fanpage überhaupt ermöglicht. Daher liegt es nahe, diese zwei Verarbeitungsvorgänge, also die Erhebung und dann die Verarbeitung zur Statistikerstellung, als eine einheitliche Vorgangsreihe zu

[420] Selbst nach dem EuGH impliziert diese Parametrierung a. nur die „Ziele[n] der Steuerung oder Förderung seiner [des Fanpage-Betreibers] Tätigkeiten".

[421] Ebenso: *Lee/Cross*, MMR 2019, 559, 562.

[422] Betrachtet man die abschließende Feststellung in EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 39, so wird dort a. zuerst die Parametrierung hinsichtlich des Zielpublikums genannt, danach die Ziele der Steuerung oder Förderung seiner Tätigkeiten. Dies könnte eine Gewichtung implizieren.

[423] Dazu: Kapitel 2 D. Mittel.

[424] Dies wird in EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 37 nicht unbedingt deutlich.

betrachten.[425] Aus der Argumentation des EuGH geht dies aber nicht ausdrücklich hervor.

Insgesamt spricht mehr dafür, in dem Urteil zu der Rechtssache Wirtschaftsakademie Entscheidungsbeiträge zu einem gemeinsamen Mittel als zu gemeinsamen Zwecken zu erkennen.[426] Dabei kann in den Parametrierungsmöglichkeiten der Fanpage eine implizite Billigung der Zwecke des Fanpage-Betreibers durch den Plattformbetreiber gesehen werden. Abseits einer solchen expliziten Billigung anhand der Parametrierungsmöglichkeiten dürfte aber auch eine Zweckkomplementarität[427] zwischen Plattformbetreiber und Fanpage-Betreiber vorliegen, da sich deren Zwecke gegenseitig bedingen. Somit wäre also auch eine wechselseitige Billigung der Zwecke aufgrund der Zweckkomplementarität impliziert. Folglich deutet das Urteil in der Rechtssache Wirtschaftsakademie auf ein ergebnisbezogenes Verständnis der gemeinsamen Entscheidung hin.

d) Fashion ID

In dem Urteil zu der Rechtssache Fashion ID[428] scheint der EuGH seinen Fokus wiederum auf die Mittel der Verarbeitung zu legen. Die gemeinsame Entscheidung über die Mittel ergebe sich für den Websitebetreiber in der Rechtssache Fashion ID daraus, dass er das Social Plugin als die Verarbeitung ermöglichendes Mittel im Wissen um seine Funktionalität eingesetzt habe.[429] Damit habe er entscheidenden Einfluss auf die Verarbeitung ausgeübt. Diese Verarbeitung wäre ohne den Einsatz des Social Plugins nicht erfolgt. Die Bedeutung dieser „entscheidenden Beeinflussung" und der unbedingten Notwendigkeit des Entscheidungsbeitrags für die Verarbeitung wird im Urteil nicht besonders klar. Denkbar ist, dass der EuGH damit eine Bagatellgrenze für Entscheidungsbeiträge von gemeinsam Verantwortlichen andeuten wollte.[430] Daneben kann man die Ermöglichung der Verarbeitung durch die Einbindung des Social Plugins seitens des Websitebetreibers auch als Entscheidung über ein wesentliches Element der Mittel verstehen, da die Ermöglichung der Verarbeitung den Kern der Entscheidung

[425] Am deutlichsten wird dies noch in: EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 38. Ähnlich scheinbar: *Kremer*, CR 2019, 676, Rn. 37 f. Ablehnend: *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 5.

[426] So a.: *Hacker*, MMR 2018, 779, 780.

[427] Dazu: Kapitel 4 E. I. 6. „Interesse" als Zweckkomplementarität.

[428] Dazu: Kapitel 4 B. III. Fashion ID.

[429] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77 f.

[430] Dazu: Kapitel 4 I. Erheblichkeitsschwelle des Entscheidungsbeitrags.

über die Mittel betrifft.[431] In jedem Fall erkennt der EuGH in der Rechtssache Fashion ID eine gemeinsame Entscheidung über die Mittel der Verarbeitung.[432]

Ob eine gemeinsame Entscheidung über die Mittel bereits ausreichend für eine gemeinsame Verantwortlichkeit ist, lässt sich auch aus der Rechtssache Fashion ID nicht klar ableiten.[433] Die Ausführungen des EuGH zu den Zwecken sind im Gegensatz zu denen zu den Mitteln vergleichsweise kurz.[434] Daraus allein lässt sich allerdings nicht schließen, dass die gemeinsame Entscheidung über die Mittel ausreichend für eine gemeinsame Verantwortlichkeit wäre. Zunächst erkennt der EuGH nicht einen gemeinsamen Zweck, sondern mehrere Zwecke der gemeinsam Verantwortlichen. So liest sich das Urteil, als sei Zweck des Websitebetreibers, mit der Einbindung des Social Plugins seine Werbung zu optimieren. Zweck des Plattformbetreibers wiederum sei die Verfügungsmöglichkeit über die verarbeiteten Daten für eigene wirtschaftliche Zwecke. Diese Zwecke der gemeinsam Verantwortlichen sollen sich gegenseitig bedingen. So sei es Bedingung für den Zweck des Websitebetreibers, in die Erhebung der personenbezogenen Daten seiner Websitebesucher durch den Plattformbetreibers einzuwilligen, der als Gegenleistung dafür das Social Plugin bereitstellt. Im Rahmen dieses Gegenleistungsverhältnisses bestehe ein beidseitiges wirtschaftliches Interesse[435] der gemeinsam Verantwortlichen. Welche Bedeutung dieses beidseitige wirtschaftliche Interesse im Hinblick etwa auf einen potenziellen gemeinsamen Zweck hat, stellt der EuGH nicht klar.[436] Ausgehend von der Kürze der Ausführungen liegt es nahe, dass im Hinblick auf die Wortwahl des EuGH – vor allem „stillschweigend [...] eingewilligt" und „Gegenleistung" – von einer jedenfalls implizierten Billigung der Zwecke auszugehen ist, anstatt von Entscheidungsbeiträgen zu einem gemeinsamen Zweck.[437]

Somit scheint der EuGH auch in der Rechtssache Fashion ID einen Entscheidungsbeitrag hinsichtlich eines Entscheidungsobjektes, hier der Mittel, verbunden mit einer Billigung eines fremden Entscheidungsbeitrags bezüglich des anderen Entscheidungsobjektes, der Zwecke, für eine gemeinsame Verantwortlichkeit ausreichen zu lassen. Dieses Verständnis der gemeinsamen Entscheidung wurde bereits

[431] Ablehnend diesbezüglich zur Rechtssache Wirtschaftsakademie: *Hacker*, MMR 2018, 779, 780.

[432] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 79.

[433] *Lee/Cross*, MMR 2019, 559, 561 interpretieren die Rechtsprechung des EuGH so, dass die Entscheidung über die Mittel bereits ausreicht.

[434] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80.

[435] Dazu: Kapitel 4 E. I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen.

[436] Kritisch: *Lee/Cross*, MMR 2019, 559, 561.

[437] Vgl. *Specht-Riemenschneider/Schneider*, GRUR Int 2020, 159, 160.

vom LG Rostock in einem Urteil aufgegriffen.[438] Dass die gemeinsame Entscheidung ergebnisbezogen und nicht prozessbezogen zu verstehen ist, wird in der Rechtssache Fashion ID auch daran deutlich, dass die Entscheidungsbeiträge der gemeinsam Verantwortlichen hinsichtlich der Mittel völlig asynchron ablaufen.[439] Der Plattformbetreiber weiß bis zum ersten Datenzufluss aufgrund des Social Plugins potenziell gar nichts von der Verarbeitung.[440] Dass entweder die entscheidende Beeinflussung – gemeint ist wohl der Entscheidungsbeitrag – der Zwecke oder der Mittel ausreicht, ergibt sich zudem implizit aus den Ausführungen des EuGH. So hält er zur gemeinsamen Entscheidung über die Mittel fest, dass einer der (gemeinsam) Verantwortlichen die Verarbeitung entscheidend beeinflusst hat.[441] Entsprechende Ausführungen mit Bezug auf die gemeinsame Entscheidung über die Zwecke fehlen hingegen.[442]

Die Schlussanträge des Generalanwalts in der Rechtssache Fashion ID[443] sind, unabhängig von einer fehlenden Bezugnahme durch den EuGH, ebenso wenig aufschlussreich. Daneben sind sie auch widersprüchlich. So will der Generalanwalt zwar zunächst eine gemeinsame Entscheidung über die Zwecke und Mittel im Sinne eines jeweiligen Entscheidungsbeitrags durch alle gemeinsam Verantwortlichen voraussetzen,[444] hält in der folgenden Randnummer aber dann fest, dass eine gemeinsame Verantwortlichkeit nicht gegeben sei, wenn der entsprechende Akteur weder über Zwecke noch Mittel der Verarbeitung entschieden habe.[445] Für die Begründung der Annahme, dass gemeinsam Verantwortliche einen Entscheidungsbeitrag zur Entscheidung sowohl über die Zwecke als auch die Mittel leisten müssen, sind die Ausführungen des Generalanwalts also nicht geeignet.[446]

e) NZÖG

In dem Urteil zu der Rechtssache NZÖG stellte der EuGH schließlich fest, dass die Mitwirkung an der Entscheidung über die Zwecke und Mittel der Verarbeitung

[438] LG Rostock, Urteil vom 15.09.2020 – 3 O 762/19 = ZD 2021, 166, Rn. 66 ff.
[439] Vgl. *Hanloser*, ZD 2019, 455, 459.
[440] Vgl. zum konsensualen Band *Hanloser*, ZD 2019, 455, 459.
[441] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 78 f.
[442] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80 f.
[443] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID).
[444] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 100.
[445] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 101. Vgl. a. die seltsame Verweisung auf WP 169 in Fn. 48, wo eine Entscheidung über Zwecke oder Mittel als ausreichend erachtet wird.
[446] Anders scheinbar: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 35.

verschiedene Formen annehmen könne.[447] Die gemeinsame Entscheidung könne entweder als gemeinsame Entscheidung oder aber auch als übereinstimmende Entscheidung erfolgen. Im Falle der übereinstimmenden Entscheidung müssten sich diese Entscheidungen aber in einer Weise ergänzen, dass sich jede von ihnen konkret auf die Entscheidung über die Verarbeitungszwecke und -mittel auswirke. Dieses Verständnis deckt sich mit den oben dargestellten prozessbezogenen[448] und ergebnisbezogenen[449] Verständnissen sowie dem Verständnis des EDPB[450]. Da das prozessbezogene Verständnis problemlos auch innerhalb des ergebnisbezogenen Verständnisses dargestellt werden kann, also bildlich gesprochen eine Teilmenge dessen darstellt, verfolgt der EuGH hinsichtlich der übereinstimmenden Entscheidung ein ergebnisbezogenes Verständnis der Entscheidung.

6. Kritik zu dem ergebnisbezogenen Verständnis der gemeinsamen Entscheidung

Häufig wird ein ergebnisbezogenes Verständnis der gemeinsamen Entscheidung dahingehend kritisiert, dass es zu einer extensiven Anwendung der gemeinsamen Verantwortlichkeit führen würde. Folglich soll die gemeinsame Verantwortlichkeit eher restriktiv verstanden werden und eine gemeinsame Entscheidung Entscheidungsbeiträge sowohl zu Zwecken als auch Mitteln erfordern. Als Argument für dieses restriktive Verständnis der gemeinsamen Entscheidung wird unter anderem auf die potenzielle Bußgeldhöhe in Art. 83 Abs. 4 lit. a DSGVO verwiesen.[451] Dieser Einwand übersieht aber, dass eine Geldbuße gem. Art. 83 Abs. 1 DSGVO unter anderem verhältnismäßig sein muss. Im Rahmen dieser Verhältnismäßigkeitsprüfung kann anhand der jeweiligen Entscheidungsbeiträge der gemeinsam Verantwortlichen eine Differenzierung hinsichtlich der Bußgeldhöhe vorgenommen werden. Daneben übersieht der Einwand dahingehend, dass den betroffenen Personen bei einem Schadensersatzanspruch gem. Art. 82 Abs. 4 DSGVO selbst bei nicht gemeinsam Verantwortlichen auch potenziell Gesamtschuldner gegenüberstehen,[452] dass diese Haftungserleichterung erst den Schadensersatz und nicht bereits die Betroffenenrechte betrifft.

[447] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 43.
[448] Kapitel 4 H. III. 1. Prozessbezogenes Verständnis der gemeinsamen Entscheidung.
[449] Kapitel 4 H. III. 2. Ergebnisbezogenes Verständnis der gemeinsamen Entscheidung.
[450] Kapitel 4 H. III. 4. c) Europäischer Datenschutzausschuss (EDPB). Der EuGH nimmt auf die Schlussanträge des Generalanwalts Bezug die wiederum auf die Leitlinien des EDPB verweisen.
[451] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, 36; *Kartheuser/Nabulsi*, MMR 2018, 717, 720.
[452] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, 36; *Kartheuser/Nabulsi*, MMR 2018, 717, 720.

Gegen ein extensives Verständnis der gemeinsamen Verantwortlichkeit wird zudem regelmäßig vorgetragen, dass aufgrund eines schwer bestimmbaren „übergeordneten" Zweckes gemeinsam Verantwortlichen eine gemeinsame Verantwortlichkeit und Haftung aufgezwungen wird, ohne dass dies für die Beteiligten selbst erkennbar sei.[453] Dabei basiert bereits die Annahme der Notwendigkeit eines gemeinsamen Zweckes aber auf einem falschen Verständnis der gemeinsamen Verantwortlichkeit.[454] Denn eine gemeinsame Verantwortlichkeit aufgrund einer Vorgangsreihe, die durch einen dermaßen schwer bestimmbaren Zweck die Verarbeitungsvorgänge verschiedener Verantwortlicher verklammert, erscheint kaum vorstellbar.[455] Allerdings kann man (und muss man wohl auch) diesen Einwand auf die bloße Notwendigkeit der Billigung eines Entscheidungsbeitrags zu Zwecken oder Mitteln einer Verarbeitung beziehen, da Kritiker der Rechtsprechung des EuGH häufig einen gemeinsamen Zweck und/oder gemeinsame Mittel für eine gemeinsame Verantwortlichkeit für erforderlich halten. Die Prüfung der Entscheidungsbeiträge eines potenziellen gemeinsam Verantwortlichen zu Zwecken oder Mitteln ist aber keine überbordende Anforderung an die beteiligten Akteure. So ist etwa die wenigstens oberflächliche Prüfung fremder Mittel, abseits der Anwendbarkeit der Haushaltsausnahme,[456] auch im Hinblick auf die generelle Compliance[457] von Verantwortlichen notwendig. Darüber hinaus sollten die Zwecke fremder Akteure relativ einfach zu erkennen sein.

Schließt man sich der Ansicht an, dass ein Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen sowohl zu den Zwecken als auch zu den Mitteln – also ein prozessbezogenes Verständnis – notwendig ist, stellt sich die Frage, was genau mit diesem Verständnis gewonnen wird. Effektiv würde dies den Anwendungsbereich der gemeinsam Verantwortlichen sehr stark begrenzen. Dies wäre rechtspolitisch gesehen aus Sicht der Verantwortlichen im Hinblick auf die Wahrnehmung der Betroffenenrechte gem. Art. 26 Abs. 3 DSGVO und die gesamtschuldnerische Haftung nach Art. 82 Abs. 4 DSGVO wohl wünschenswert. Andererseits wäre die gegenseitige Einbindung gemeinsam Verantwortlicher in die jeweilige Entscheidung über Zwecke und Mittel häufig ein Formalismus, wenn Sinn einer Kollaboration doch

[453] *Kartheuser/Nabulsi*, MMR 2018, 717, 719.

[454] Dazu: Kapitel 4 E. I. Das „Interesse" in der Rechtssache Fashion ID als Zweckkomplementarität der gemeinsam Verantwortlichen und Kapitel 4 E. II. Die „Einwilligung" in eine Verarbeitung als Einigung auf einen gemeinsamen Zweck?

[455] Vgl. zur Klammerwirkung der Vorgangsreihe *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 25 Beispiel 10.

[456] Dazu: Kapitel 5 I. Haushaltsausnahme.

[457] Etwa im Hinblick auf Urheberrecht, Patentrecht und Geschäftsgeheimnisse.

gerade die Arbeitsteilung ist. Daneben wäre der Nachweis eines entsprechenden Entscheidungsbeitrags, abseits rechtlicher oder vertraglicher Fixierung, regelmäßig schwierig zu erbringen. Grundsätzlich könnten Betroffenenrechte zwar auch gegenüber verschiedenen singulären Verantwortlichen – statt gemeinsamen – geltend gemacht werden. Allerdings sind durchaus Szenarien denkbar, in denen keine separaten singulären Verantwortlichkeiten gebildet werden können.[458] Sofern in diesen Szenarien nicht über Zwecke und Mittel insgesamt entschieden werden kann, ohne dass Verarbeitungen auch arbeitsteilig durchgeführt werden, ist ein extensives Verständnis der gemeinsamen Entscheidung im Sinne des ergebnisbezogenen Verständnisses zwingend.[459]

7. Antizipierte Entscheidungsbeiträge?

Eng verbunden mit der Frage, ob die gemeinsame Entscheidung prozess- oder ergebnisbezogen zu verstehen ist, ist auch die Frage, ob die einzelnen Entscheidungsbeiträge zeitlich versetzt erfolgen können. Ein prozessbezogenes Verständnis der gemeinsamen Entscheidung würde voraussetzen, dass Entscheidungsbeiträge im Hinblick auf die Einigung noch nicht abgeschlossen sind und in engem zeitlichem Zusammenhang erfolgen, während ein ergebnisbezogenes Verständnis auch abgeschlossene Entscheidungsbeiträge mit weitem zeitlichen Abstand erfassen würde. Demnach könnten ergänzende Entscheidungsbeiträge noch unbekannter gemeinsam Verantwortlicher antizipiert werden. Da in letzterem Falle die Entscheidungsbeiträge des antizipierenden gemeinsam Verantwortlichen unveränderlich sind, wird der Entscheidungsspielraum des anderen gemeinsam Verantwortlichen häufig nur in einem Eingehen auf das „Angebot" oder dessen – datenschutzrechtlich irrelevantes – Übergehen bestehen.[460] In diesem Sinne kann ein Akteur ein weitestgehend fertiges Entscheidungspaket vorlegen, das von anderen Akteuren nur noch um wenige, aber dafür notwendige Entscheidungsbeiträge ergänzt wird. *Wagner* spricht hierbei von einer abstrakten und konkreten Festlegung der Beteiligten oder auch von zwei sich gegenseitig bedingenden Einwirkungssphären.[461] Dabei dürfte aufgrund der Antizipation des Entscheidungsbeitrags des nachfolgenden Akteurs häufig nur die Möglichkeit bestehen einen, für die Verarbeitung gleichwohl notwendigen, Entscheidungsbeitrag zu den Mitteln zu leisten. Die Zwecke des

[458] Vgl. etwa *Monreal*, CR 2019, 797, Rn. 49.
[459] *Kremer*, CR 2019, 225, Rn. 18.
[460] Dazu: Kapitel 4 I. Erheblichkeitsschwelle des Entscheidungsbeitrags.
[461] *Wagner*, ZD 2018, 307, 309 f.

antizipierenden Akteurs hingegen sind bei Durchführung der Verarbeitung logischerweise bereits festgelegt, so dass der nachfolgende Akteur sich diese nur zu-eigen-machen kann oder eigene Zwecke verfolgt. Deutlich wird die Antizipation von Entscheidungsbeiträgen in den Rechtssachen Wirtschaftsakademie[462] sowie Fashion ID[463]. Dort stellte der Plattformbetreiber Infrastruktur[464] bereit, die unter vorformulierten Konditionen genutzt werden kann. Ein individuelles Aushandeln der Bedingungen fand dabei nicht statt, es handelte sich vielmehr um automatisierte Angebote von Infrastruktur. Sofern man solche Szenarien als gemeinsame Verantwortlichkeit erfassen will, scheint auch deshalb ein ergebnisbezogenes Verständnis der gemeinsamen Entscheidung notwendig. Generell dürften Anwendungsfälle von antizipierten Entscheidungsbeiträgen regelmäßig die Bereitstellung von Infrastruktur oder Daten sein.

8. Unbewusste Entscheidungsbeiträge?

Daneben ist fraglich, inwiefern eine gemeinsame Entscheidung die Kenntnis der anderen gemeinsam Verantwortlichen oder den Willen zur Zusammenarbeit mit diesen voraussetzt.[465] Dieser Mangel an Kenntnis oder Wille wird teilweise als Argument gegen die Möglichkeit antizipierter Entscheidungsbeiträge vorgebracht.[466] Dabei wird allerdings unterschlagen, dass die Verantwortlichkeit grundsätzlich keine spezifischen Kenntniselemente voraussetzt.[467] Andeutungen der Notwendigkeit einer solchen Kenntnis könnte man maximal einer Randnummer in der Rechtssache Fashion ID entnehmen.[468] Mangels weiterer Bezugnahme durch den EuGH dürfte es sich dabei aber eher um ein obiter dictum als ratio decidendi handeln. Ob die Kenntnis der anderen gemeinsam Verantwortlichen oder der Wille zur Zusammenarbeit anderweitig hergeleitet werden können, ist zweifelhaft. Die Auftragsverarbeitung nach Art. 28 Abs. 1 DSGVO lässt sich hierfür nicht heranziehen, denn das Konzept der

[462] Unterstellt Facebook prüft nicht jede einzelne Eröffnung einer Facebook-Seite: EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 32.

[463] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77.

[464] In der Rechtssache Wirtschaftsakademie eine vorkonfigurierte Webseite, in der Rechtssache Fashion ID Programmcode in Form eines Social Plugins.

[465] Zu Kenntniselementen hinsichtlich der Entscheidung bzw. des Entscheidungsbeitrags: Kapitel 2 E. I. Vorfrage: Notwendige Kenntniselemente der Entscheidung.

[466] *Moos/Rothkegel*, MMR 2019, 584, 585 f. Kritisch a.: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 51.

[467] *Weichert*, ZD 2014, 605, 606.

[468] Spezifisch: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77: „[...] in ihre Website offenbar im Wissen eingebunden hat, dass dieser als Werkzeug zum Erheben und zur Übermittlung von personenbezogenen Daten [...] dient".

Auftragsverarbeitung basiert, wie der Name bereits impliziert, auf einer bewussten Entscheidung, eine externe Stelle einzubinden. Diese bewusste Entscheidung greift für die gemeinsame Verantwortlichkeit gerade nicht, da sie aufgrund der faktischen Umstände besteht. Legen Verantwortliche die Zwecke und Mittel einer Verarbeitung gemeinsam fest, so sind sie gemeinsam Verantwortliche. Versteht man „gemeinsam" zudem, wie ausgeführt,[469] als „mit anderen", liegt eine Kenntnis der anderen gemeinsam Verantwortlichen vom Telos ausgehend nicht unbedingt nahe. Auch die bei einer gemeinsamen Verantwortlichkeit notwendige Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO ist zwar eine Pflicht der gemeinsam Verantwortlichen. Sie ist aber nicht konstitutiv für die gemeinsame Verantwortlichkeit. Daher kann man sie in gewisser Weise als „Obliegenheit" der Verantwortlichen begreifen, da die Konsequenz einer fehlenden Vereinbarung unklare interne Zuständigkeiten sowie potenziell die Verhängung einer Geldbuße gem. Art. 83 Abs. 4 lit. a DSGVO sind.[470]

IV. Fazit

Im Hinblick auf den Wortlaut der Definition in Art. 4 Nr. 7 und Art. 26 Abs. 1 S. 1 DSGVO, die Position der Aufsichtsbehörden und die Rechtsprechung des EuGH scheint ein ergebnisbezogenes Verständnis der gemeinsamen Entscheidung nicht nur möglich, sondern naheliegend. Auch systematisch und teleologisch ist es sinnvoll, nicht einen gemeinsamen Einigungsprozess vorauszusetzen, da dies den Anwendungsbereich der gemeinsamen Verantwortlichkeit stark einengen würde.[471] Trotz der Möglichkeit eines Entscheidungsbeitrags alternativ zu Zwecken oder Mitteln der Verarbeitung seitens eines individuellen gemeinsam Verantwortlichen bedeutet das ergebnisbezogene Verständnis aber dennoch, dass als Ergebnis der Entscheidungsbeiträge aller gemeinsam Verantwortlicher eine Entscheidung über alle notwendigen Elemente der Zwecke und Mittel der Verarbeitung vorliegen muss. Daneben müssen die Elemente der Zwecke und Mittel der Verarbeitung, zu denen kein Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen vorliegt, durch diesen gemeinsam Verantwortlichen gebilligt werden.[472] Liegen also aufgrund des Entscheidungsbeitrags eines individuellen gemeinsam Verantwortlichen gemeinsame Zwecke vor, müsste eine Billigung dessen hinsichtlich divergierender Mittel der

[469] Dazu: Kapitel 4 C. II. Unmittelbarer Kontext: „mit anderen".
[470] Vgl. Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, 24.
[471] *Monreal*, CR 2019, 797, Rn. 40.
[472] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung; ähnlich: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 51; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 42 in der Zusammenfassung der EuGH-Kriterien.

anderen gemeinsam Verantwortlichen vorliegen. Liegen andererseits gemeinsame Mittel aufgrund seines Entscheidungsbeitrags vor, müsste eine Billigung der divergierenden Zwecke der anderen gemeinsam Verantwortlichen vorliegen. Liegen weder gemeinsame Zwecke noch gemeinsame Mittel vor, dürfte es sich bei der Beziehung zwischen mehreren Akteuren häufig nur um eine reine Übermittlung von personenbezogenen Daten handeln.[473] Daneben können, sofern sich die Verarbeitungsvorgänge hinreichend abgrenzen lassen, schlicht auch separate Verantwortlichkeiten vorliegen.[474]

Neben diesen rein faktischen Voraussetzungen der gemeinsamen Entscheidung ist weder die Vereinbarung[475] nach Art. 26 Abs. 1 S. 2 DSGVO noch die Eigenbezeichnung der Akteure konstitutiv für eine Einordnung als gemeinsam Verantwortliche. Die Analyse der gemeinsamen Verantwortlichkeit erfolgt allein anhand der tatsächlichen Verhältnisse.[476] Eigenbezeichnungen oder vertragliche Vereinbarungen können insoweit nur eine Indizwirkung entfalten.[477]

I. Erheblichkeitsschwelle des Entscheidungsbeitrags

Ausgehend von der Feststellung, dass ein Entscheidungsbeitrag alternativ zu den Zwecken oder Mitteln (im weiteren Sinne[478]) – je nachdem welches der Entscheidungsobjekte als gemeinsames Element vorliegt – ausreichend für eine gemeinsame Entscheidung ist, stellt sich die Frage, ob hinsichtlich dieses Entscheidungsbeitrags noch eine qualitative oder quantitative Einschränkung gilt oder jeder (scheinbar) noch so triviale Entscheidungsbeitrag ausreicht.[479] Eine qualitative Einschränkung des Entscheidungsbeitrags würde darauf abstellen, auf welches Entscheidungsobjekt, also Zwecke oder Mittel, oder welches Element dieser Entscheidungsobjekte ein Entscheidungsbeitrag abzielt. Eine quantitative Einschränkung des Entscheidungsbeitrags würde sich darauf

[473] Vgl. *Kartheuser/Nabulsi*, MMR 2018, 717, 719. Ähnlich: Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 9. Zur Kettenübermittlung siehe: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24.

[474] Vgl. die separate Verantwortlichkeit des Suchmaschinenbetreibers in EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 25 ff.

[475] Noch in der 2. Aufl. explizit: Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 10; Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 72; unklar: Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 4.

[476] G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 33, 38.

[477] Vgl. *Söbbing*, ITRB 2020, 218, 220 f.

[478] Also abseits der Identität der Verarbeitung aufgrund der verarbeiteten Daten.

[479] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 23.

beziehen, wie stark der Einfluss des Entscheidungsbeitrags auf die Verarbeitung ist. Die Kontrollüberlegung wäre also, inwieweit sich der Verarbeitungsvorgang ohne diesen Entscheidungsbeitrag anders darstellen würde. Daneben ist zu bedenken, inwiefern der Entscheidungsspielraum eines Akteurs Berücksichtigung bei der Erheblichkeitsschwelle findet und ob auch ein Unterlassen als Entscheidungsbeitrag gewertet werden kann. Insgesamt stellt sich die Frage, ob es eine Erheblichkeitsschwelle für den Entscheidungsbeitrag eines gemeinsam Verantwortlichen gibt.

I. Negative Konstruktion der Erheblichkeitsschwelle

Sofern man sich die Trias der Verantwortlichkeitsrollen in der DSGVO vor Augen führt – Verantwortlicher, Auftragsverarbeiter oder eben keine Verantwortlichkeit – lässt sich die Erheblichkeitsschwelle des Entscheidungsbeitrags negativ konstruieren. Denn ein Auftragsverarbeiter darf, ohne gem. Art. 28 Abs. 10 DSGVO zum Verantwortlichen zu werden, nur über die unwesentlichen Elemente der Mittel[480] der Verarbeitung entscheiden, da er gem. Abs. 1[481] für die technischen und organisatorischen Maßnahmen der Verarbeitung zuständig ist. Dieser eingeschränkte Spielraum ergibt sich im Umkehrschluss auch aus den Festlegungserfordernissen – eben denen für den Verantwortlichen – aufgrund des durch die Auftragsverarbeitung bedingten Vertrags nach Art. 28 Abs. 3 DSGVO.[482] Diese Festlegungserfordernisse, als wesentliche Elemente der Mittel, beinhalten unter anderem, welche Daten verarbeitet werden (Abs. 3), wie lange Daten verarbeitet werden (Abs. 3), wann sie gelöscht werden (Abs. 3 i.V.m. lit. g) und wer zu ihnen Zugang hat (Abs. 3 lit. b i.V.m. Art. 29 DSGVO).[483] Wesentliche Elemente der Mittel scheinen also vor allem solche zu sein, die die Daten an sich und nicht die Verarbeitung im weiteren Sinne betreffen. Auch im Verständnis der Art. 29-Datenschutzgruppe sollen technische und organisatorische Fragen der Verarbeitung nicht als wesentliche Elemente der Verarbeitung verstanden werden.[484]

---

[480] In Abgrenzung zu den wesentlichen Elementen der Mittel nach *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[481] Siehe a. Art. 28 Abs. 3 lit. e DSGVO.

[482] Unabhängig davon wäre im Hinblick auf eine bessere Verständlichkeit der Norm allerdings eine differenzierte Systematisierung der Mittel, wie sie die Art. 29-Datenschutzgruppe vornimmt, bereits bei den Legaldefinitionen wünschenswert.

[483] Dazu: Kapitel 2 D. Mittel; Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[484] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

Der Verantwortliche hingegen muss, im Umkehrschluss zum Auftragsverarbeiter, über die Zwecke und die wesentlichen Elemente der Mittel der Verarbeitung entscheiden. Bei einer gemeinsamen Verantwortlichkeit muss also als Ergebnis der Kollaboration über die Zwecke und wesentlichen Elemente der Mittel der Verarbeitung entschieden sein. Ohne einen Auftragsverarbeiter, der an der Verarbeitung der gemeinsam Verantwortlichen beteiligt ist, muss aber auch über die unwesentlichen Elemente der Mittel durch die gemeinsam Verantwortlichen entschieden werden. Die Erheblichkeitsschwelle des Entscheidungsbeitrags eines gemeinsam Verantwortlichen ist, soweit kein Auftragsverarbeiter beteiligt ist, also bereits dann erreicht, wenn dieser Entscheidungsbeitrag ein unwesentliches Element der Mittel betrifft. Denn dieser Entscheidungsbeitrag kann dann keinem Auftragsverarbeiter zugerechnet werden. Somit bestünde für diesen Entscheidungsbeitrag ansonsten insgesamt kein Zuordnungssubjekt. Sofern ein Auftragsverarbeiter an einer Verarbeitung gemeinsam Verantwortlicher beteiligt ist, muss daher bei einem Entscheidungsbeitrag zu einem unwesentlichen Element der Mittel auch geprüft werden, ob dieser Entscheidungsbeitrag von einem Auftragsverarbeiter, also einem grundsätzlich weisungsgebundenen Beteiligten stammt oder aber von einem gemeinsam Verantwortlichen.

Trägt ein Akteur in irgendeiner Weise zu einer Verarbeitung bei, muss somit festgestellt werden, ob der Beitrag die Schwelle des Art. 28 Abs. 10 DSGVO bzw. Art. 4 Nr. 7 DSGVO überschreitet, indem zu zumindest einem Aspekt der Zwecke oder wesentlichen Elemente der Mittel der Verarbeitung beigetragen wird und falls dies nicht der Fall ist, ob eine Weisungsgebundenheit gegenüber einem Verantwortlichen vorliegt. Liegt ein Beitrag vor, der die Zwecke oder wesentliche Elemente der Mittel beeinflusst, ist keine Auftragsverarbeitung mehr denkbar und im Rahmen der Verantwortlichkeitsrollen mangels Alternativen nur ein (gemeinsam) Verantwortlicher möglich.[485] Handelt es sich hingegen um einen Beitrag zu den unwesentlichen Elementen der Mittel, muss zusätzlich geprüft werden, ob eine Weisungsgebundenheit des Akteurs besteht.

[485] Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 51: „Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that **characterize** a controller are decided by more than one party." (Hervorhebung durch den Autor).

II. Qualitative Einschränkungen im Hinblick auf die Erheblichkeitsschwelle

Neben dieser negativen Konstruktion der Erheblichkeitsschwelle lässt sich erwägen, ob das genaue Bezugsobjekt des Entscheidungsbeitrags, also Zwecke oder Mittel bzw. Teilaspekte hiervon, eine bestimmte Gewichtung des Entscheidungsbeitrags im Hinblick auf die Erheblichkeitsschwelle zur Folge hat. Aus den eben genannten Erwägungen kann zunächst abgeleitet werden, dass ein Akteur, der einen Entscheidungsbeitrag zu den Zwecken beisteuert, immer als gemeinsam Verantwortlicher zu erachten ist.[486] Ebenso ist ein Akteur, der einen Entscheidungsbeitrag zu den wesentlichen Elementen der Mittel beisteuert, immer als gemeinsam Verantwortlicher zu werten.

Problematisch erscheint hingegen die Situation, wenn keine Weisungsgebundenheit eines Akteurs vorliegt, aber auch kein Entscheidungsbeitrag zu den Zwecken oder wesentlichen Elementen der Mittel geleistet wird, sondern nur zu den unwesentlichen Elementen der Mittel. Gem. Art. 4 Nr. 7 DSGVO müsste es sich dann um einen (gemeinsam) Verantwortlichen handeln, da die Definition des Verantwortlichen nicht zwischen wesentlichen und unwesentlichen Elementen der Mittel, im Sinne der Art. 29-Datenschutzgruppe,[487] unterscheidet. Die Definition des singulären Verantwortlichen in Art. 4 Nr. 7 DSGVO muss diese Unterscheidung aber auch gar nicht treffen, da ohnehin nur ein Akteur entscheidet. Die Definition der gemeinsam Verantwortlichen in Art. 26 Abs. 1 S. 1 DSGVO trifft allerdings ebenso keine Unterscheidung zwischen wesentlichen und unwesentlichen Elementen der Mittel. Selbst der Auftragsverarbeiterexzess in Art. 28 Abs. 10 DSGVO setzt die Unterscheidung zwischen wesentlichen und unwesentlichen Elementen nicht explizit voraus. Diese Unterscheidung ergibt sich vielmehr systematisch aus Art. 28 Abs. 3 DSGVO und setzt dann notwendigerweise eine Auftragsverarbeitung, also auch die Weisungsgebundenheit eines Akteurs, voraus. Damit es bei fehlender Weisungsgebundenheit eines Akteurs nicht zu einem Schutzdefizit für die betroffenen Personen kommt, da es ja keine Auftragsverarbeitung ohne Weisung gibt,[488] muss hier de lege lata ein Verantwortlicher angenommen werden.[489] Diesen nicht

[486] Vgl. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9.

[487] Dazu: Kapitel 2 D. Mittel.

[488] Die Auftragsverarbeitung ist im Gegensatz zur gemeinsamen Verantwortlichkeit streng hierarchisch konzipiert, wie die Figur des Unterauftragsverarbeiters aus Art. 28 Abs. 4 DSGVO belegt.

[489] Anders wohl Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 21, der eine bloße Zusammenarbeit nicht als gemeinsame Verantwortlichkeit mangels „kooperativer Determinierung des Zielzustandes" werten will.

weisungsgebundenen Akteur, der nur einen Entscheidungsbeitrag zu den unwesentlichen Elementen der Mittel beisteuert, scheinen die aufsichtsbehördlichen Gremien[490] bislang nicht erkannt zu haben. Denn sie verlangen für den Verantwortlichen und damit auch für gemeinsam Verantwortliche eine Entscheidung über wesentliche Elemente der Mittel.[491]

Softwarehersteller etwa entscheiden häufig durch die Standardkonfiguration ihrer Software über bestimmte Aspekte der Mittel, teilweise auch über wesentliche Elemente der Mittel. Nach dem Willen des Unionsgesetzgebers sollen Hersteller aber gerade nicht von der DSGVO erfasst werden.[492] Erfasst werden vielmehr erst die Verwender von Software, die häufig nicht die notwendige Sachkenntnis für die entsprechende Konfiguration mitbringen. Sofern der Verwender einer Software deren Konfiguration im Hinblick auf die Mittel bei der ersten Verwendung der Software vornimmt, ist diese ihm dann unproblematisch zuzurechnen. Mangels Anwendung der DSGVO auf die Hersteller gilt diese Zurechnung allerdings auch dann, wenn der Verwender über die Verwendung hinaus keinerlei Konfiguration vornehmen muss. Diese Verantwortlichkeit trifft auch jeden anderen Akteur, der über die Konfiguration der Software oder deren Verwendung entscheidet, unabhängig vom konkreten Beteiligungsgrad an der Verarbeitung. Sofern solche Akteure nicht Auftragsverarbeiter sind, gelten für sie dann notwendigerweise alle Pflichten und Haftungsrisiken eines Verantwortlichen. Denkbar erscheint eine Beteiligung, bei der nur über unwesentliche Elemente der Mittel entschieden wird, vor allem im Bereich von IT-Dienstleistungen. Denn jede Art der Konfiguration, des Supports oder der Wartung der Verarbeitungssoft- und Hardware, also der Entscheidung über unwesentliche Elemente der Mittel, erfordert de lege lata eine Auftragsverarbeitung. Der Dienstleister muss sich also der Weisungsgebundenheit gegenüber dem Verantwortlichen unterwerfen und grundsätzlich einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO abschließen. Damit werden kurzfristige und niederschwellige Dienstleistungen aufgrund des immanenten Verantwortlichkeitsrisikos des Dienstleisters faktisch verhindert und die Auftragsverarbeitung erhält zunehmend Züge einer reinen Förmelei.

---

[490] Also Art. 29-Datenschutzgruppe, EDPS sowie EDPB.

[491] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17; *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 9 f.; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40.

[492] Dazu: Kapitel 5 G. Herstellerverantwortlichkeit.

Bei der alleinigen Entscheidung über unwesentliche Elemente der Mittel zeigt sich aber ein auffälliges Missverhältnis von Entscheidungsbeitrag und Verantwortlichkeit. Sinnvoller erscheint de lege ferenda eine Abstufung der Verantwortlichkeit im Sinne einer datenschutzrechtlichen Beihilfe,[493] die einerseits mangels Weisungsgebundenheit zwar weitergehender als die Auftragsverarbeitung einzuordnen wäre, andererseits mangels Entscheidungskompetenz über die Zwecke und die wesentlichen Elemente der Mittel allerdings nicht zur Einordnung als Verantwortlicher führen würde. Diese Abstufung scheint auch im Hinblick auf das Risiko für das eigentliche Schutzobjekt der DSGVO, die personenbezogenen Daten, sinnvoll. Eine Entscheidungskompetenz des nicht weisungsgebundenen Quasi-Auftragsverarbeiters im Hinblick auf technische oder organisatorische Maßnahmen, die eben nicht Kernfragen des Umgangs mit den personenbezogenen Daten betreffen, mag zwar organisatorisch – mangels Weisungsgebundenheit – risikobehafteter sein, inhaltlich ist sie allerdings vergleichbar riskant.

Die Untergrenze eines Entscheidungsbeitrags für eine gemeinsame Entscheidung liegt also in einem Beitrag, der die Zwecke oder Mittel der Verarbeitung betrifft[494] und, sofern eine Weisungsgebundenheit besteht, die Grenzen der Entscheidungsautonomie des Auftragsverarbeiters überschreitet,[495] also nicht nur unwesentliche Elemente der Mittel betrifft.[496] Mangels entsprechender Verantwortlichkeitskonzepte muss sich aber auch ein Akteur, dessen Entscheidungsbeitrag sich qualitativ auf der Höhe einer Auftragsverarbeitung bewegt, der andererseits aber nicht weisungsgebunden ist, de lege lata als gemeinsam Verantwortlicher einordnen lassen. Sofern die gemeinsame Verantwortlichkeit also dahingehend kritisiert wird, dass bereits äußerst geringe Entscheidungsbeiträge oder Einflussmöglichkeiten sie begründen,[497] ist dies vor allem der Unterkomplexität der Verantwortlichkeitskonzepte geschuldet.

---

[493] Dazu: Kapitel 5 F. „Datenschutzrechtliche Beihilfe".

[494] Vgl. *Lezzi/Oberlin*, ZD 2018, 398, 400, die aber einen Beitrag sowohl zu Zweck als a. Mittel fordern. Ebenso: Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 12.

[495] Denn dann liegt ein Auftragsverarbeiterexzess vor, dazu: Kapitel 4 K. Auftragsverarbeiterexzess und Mitarbeiterexzess.

[496] Siehe zum Verzicht auf eine qualitative Einschränkung der Entscheidungsgewalt a.: Grabitz/Hilf[40]/*Brühann*, A 30 Art. 2 DSRL, Rn. 19.

[497] So etwa: *Kartheuser/Nabulsi*, MMR 2018, 717, 719.

III. Quantitative Einschränkungen im Hinblick auf die Erheblichkeitsschwelle

Eine quantitative Einschränkung des Entscheidungsbeitrags würde hingegen daran anknüpfen, inwieweit ein Entscheidungsbeitrag die Verarbeitung beeinflusst, also ob die Verarbeitung durch diesen Entscheidungsbeitrag maßgeblich anders ausfällt. Vor dem Urteil des EuGH in der Rechtssache Wirtschaftsakademie schien, jedenfalls in Deutschland, die Auffassung vorzuherrschen, dass eine gemeinsame Verantwortlichkeit eine nahezu paritätische Beteiligung von Verantwortlichen voraussetzen würde.[498] Demnach sollte bei einem klar überwiegenden Einfluss eines Akteurs diesem die alleinige Verantwortlichkeit zugewiesen werden. Das Erfordernis einer hinreichenden Beteiligung, im Sinne eines Entscheidungsbeitrags, für eine gemeinsame Verantwortlichkeit lässt sich allerdings weder aus Art. 4 Nr. 7 DSGVO noch Art. 26 Abs. 1 S. 1 DSGVO herleiten.[499] Daher stellte der EuGH in der Rechtssache Wirtschaftsakademie auch klar: „[...] können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist."[500]

Die Orientierung des Umfangs der Verantwortlichkeit an den jeweils maßgeblichen individuellen Verarbeitungsvorgängen wird in der Literatur als vorgangsorientierter Ansatz bezeichnet.[501] Seine weitere Ausformung erfuhr der Ansatz in dem Urteil in der Rechtssache Fashion ID.[502] Dort stellte der EuGH fest, dass die gemeinsame Verantwortlichkeit immer anhand eines konkreten Verarbeitungsvorgangs, über dessen Zwecke und Mittel entschieden wird, analysiert werden muss. *Hanloser* versteht diesen vorgangsorientierten Ansatz und die damit verbundene Beschränkung der gemeinsamen Verantwortlichkeit auf einzelne Vorgänge bzw. Vorgangsreihen als Korrektiv dafür, dass keine Parität der Entscheidungsmacht[503] bei gemeinsam

[498] Vgl. etwa Simitis/*Dammann*, § 3 BDSG a.F., Rn. 224; *Alich/Nolte*, CR 2011, 741, 743.

[499] Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 9; *Kremer*, CR 2019, 225, Rn. 16; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22. Ähnlich: *Kartheuser/Nabulsi*, MMR 2018, 717, 720; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 28 f.

[500] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 43. Bestätigt in: EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 66.

[501] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[502] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74.

[503] Als Summe der Entscheidungsbeiträge.

Verantwortlichen verlangt wird.[504] Diese Interpretation scheint aber konstruiert, da der EuGH nur den Einfluss eines Akteurs auf bestimmte Vorgänge betrachtet und nicht hinsichtlich eines Idealtypus des gemeinsam Verantwortlichen korrigiert. Der EuGH macht also keine Gesamtrechnung der Beteiligung eines Akteurs an verschiedenen Vorgängen auf. Dass es im Rahmen vernetzter oder mehrstufiger Anbieterverhältnisse[505] nicht nur zu paritätischen Entscheidungskonstellationen kommen kann, sollte eigentlich selbstverständlich sein. Denkbar sind vielmehr verschiedenste Beteiligungs- und somit auch quantitative Entscheidungsbeitragsformen.

Will man neben der qualitativen Einschränkung des Entscheidungsbeitrags auch eine quantitative Einschränkung de lege ferenda einführen, stellt sich die Frage, wie der Entscheidungsbeitrag überhaupt quantitativ zu ermitteln wäre. Dabei auf den Verantwortlichkeitsgrad[506] des individuellen gemeinsam Verantwortlichen abzustellen, würde einen Zirkelschluss darstellen, da dieser Grad erst im Rahmen der gemeinsamen Verantwortlichkeit überhaupt ermittelbar wäre. Daneben ist der Verantwortlichkeitsgrad auch nur eine Agglomeration der verschiedenen Entscheidungsbeiträge, die als solche gerade in multilateralen, wechselseitigen, komplexen Verarbeitungsszenarien kaum noch präzise zu bestimmen sein dürften.[507] Ausreichend ist also bereits ein minimaler Entscheidungsbeitrag zu den Zwecken oder Mitteln der Verarbeitung.[508]

IV. Der Entscheidungsspielraum als Voraussetzung für einen Entscheidungsbeitrag

Fraglich erscheint weiterhin, ob für den Entscheidungsbeitrag eines gemeinsam Verantwortlichen ein Entscheidungsspielraum bestehen muss und falls ja, welche Anforderungen an diesen zu stellen sind. Bisweilen wird kritisiert, dass bestimmte Akteure im Rahmen ihrer Entscheidung keinen hinreichenden Entscheidungsspielraum hätten und damit auch kein berücksichtigungsfähiger

[504] *Hanloser*, ZD 2019, 455, 459.

[505] Zum Begriff: BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 439. Zu weiteren Beispielen einer praktischen Ausdifferenzierung der Beteiligungsformen: *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 504.

[506] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[507] Vgl. zur Verantwortungsermittlungsdiffusion *Augsberg*, RW 2019, 109, 114 f.

[508] *Monreal*, CR 2019, 797, Rn. 41; *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 70 f.; ähnlich: *Lezzi/Oberlin*, ZD 2018, 398, 400, die dies allerdings bezüglich der Zwecke und Mittel verlangen.

Entscheidungsbeitrag vorliegen könne.[509] Es würde beispielsweise kein inhaltlicher Einfluss auf die Verarbeitung ausgeübt und die Verarbeitung könnte entweder nur ermöglicht oder verhindert werden. Besonders deutlich wird ein eingeschränkter Entscheidungsspielraum in Verarbeitungsszenarien, in denen Entscheidungsbeiträge antizipiert werden,[510] etwa in dem Sachverhalt in der Rechtssache Fashion ID.[511] Hier hatte der Websitebetreiber nur die Möglichkeit den Programmcode des Social Plugin, so wie er war, einzubinden. Im Gegensatz zum Sachverhalt in der Rechtssache Wirtschaftsakademie[512] war keine weitere Parametrierung der Mittel, also des Social Plugins, möglich. Inwiefern diese Parametrierung überhaupt die Verarbeitung der ohnehin bereits erhobenen Daten zur Statistik maßgeblich beeinflusste, sei dahingestellt. Es handelte sich mit anderen Worten jedenfalls um die Annahme oder Ablehnung eines inhaltlich unverhandelbaren Angebots.

Diese Kritik übersieht aber, dass ein Entscheidungsspielraum bereits bei einer rein binären, also beispielsweise einer ja/nein-Entscheidung besteht.[513] So weist v*an Alsenoy* darauf hin, dass auch im Falle einer „take-it-or-leave-it"-Situation[514] im Rahmen der Ermöglichung einer Verarbeitung ein Minimum an Entscheidungsmacht über die Mittel der Verarbeitung besteht.[515] Die Ermöglichung einer Verarbeitung wiederum stellt eine conditio-sine-qua-non-Bedingung für diese Verarbeitung dar. Daher lässt sich hinterfragen, inwiefern dies nicht vielmehr das Maximum einer tatsächlichen Beeinflussung der Verarbeitung darstellt, unabhängig von einer weiteren inhaltlichen Beeinflussung der Zwecke oder Mittel.[516] Zudem kann man die Ermöglichung einer Verarbeitung als Entscheidung über die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie den Zugang zu personenbezogenen Daten

[509] So etwa: *Moos/Rothkegel*, MMR 2019, 584, 586.

[510] Dazu: Kapitel 4 H. III. 7. Antizipierte Entscheidungsbeiträge?

[511] Dazu: Kapitel 4 B. III. Fashion ID.

[512] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[513] *Wagner*, ZD 2018, 307, 309; vgl. *Hanloser*, ZD 2019, 455, 459: „[...] können [...] nur entweder einbinden oder davon absehen." Siehe a. die Ausführungen der Art. 29-Datenschutzgruppe zur Ausfertigung von Vertragsbedingungen durch Auftragsverarbeiter: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 32 sowie Beispiel 22 ebd., 35.

[514] Vgl. *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 91.

[515] *Alsenoy*, CLSR[28] (2012), 25, 31, 33. Ähnlich: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 51.

[516] So stellt etwa die Art. 29-Datenschutzgruppe hinsichtlich des Zweckes die Frage, wer die Verarbeitung veranlasst: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11; ähnlich *Brühann*, DuD[28] (2004), 201, 204 mit Verweis auf Veranlassung und die Bestimmung wesentlicher Merkmale. *Nebel*, RdV 2019, 9, 11 m.w.N. inwiefern a. in der Ermöglichung eine Entscheidung über Zwecke und Mittel vorliegt. *Wagner*, ZD 2018, 307, 309 spricht von zwei sich gegenseitig bedingenden Einwirkungssphären. Überaus kritisch zur Ermöglichung: *Schleipfer*, CR 2019, 579, 580 f.

verstehen. Damit läge ein Entscheidungsbeitrag zu wesentlichen Elementen der Mittel vor.[517] Für die Entscheidung eines gemeinsam Verantwortlichen reicht also ein rein binärer Entscheidungsspielraum, von dem auch die reine Ermöglichung einer Verarbeitung erfasst wird.[518]

V. Unterlassen als Entscheidungsbeitrag?

Im Rahmen der quantitativen Einschränkung eines Entscheidungsbeitrags ist zudem fraglich, ob ein Entscheidungsbeitrag durch Unterlassen erfolgen kann.[519] Im Hinblick auf die Urteile des EuGH lässt sich bislang immer ein aktives Verhalten der gemeinsam Verantwortlichen erkennen. So hatte der Plattformbetreiber in der Rechtssache Wirtschaftsakademie die Infrastruktur für Fanpages bereitgestellt, der Fanpage-Betreiber hingegen die konkrete Fanpage eingerichtet. In der Rechtssache Fashion ID hatte der Plattformbetreiber den Programmcode für das Social Plugin zur Verfügung gestellt, der Websitebetreiber wiederum diesen Code eingebunden. In der Rechtssache Jehovan todistajat hatte die Glaubensgemeinschaft die Verkündigungstätigkeit ihrer Mitglieder organisiert, die Mitglieder wiederum hatten die konkreten Datenverarbeitungen durchgeführt. Aus den Rechtssachen Wirtschaftsakademie und Fashion ID lässt sich deutlich ableiten, dass die Entscheidungsbeiträge von den gemeinsam Verantwortlichen kumulativ nötig waren, damit es zu einer Verarbeitung kommt. Diese „conditio sine qua non"-Konditionalität scheint bei der Rechtssache Jehovan todistajat nicht offensichtlich gegeben. So unterstützt die Einteilung der Verkündigungstätigkeit der Mitglieder in Bezirke,[520] als Organisation und Koordination der Verkündigungstätigkeit seitens der Gemeinschaft, zwar die Mitglieder, unbedingt notwendig ist sie aber nicht für deren Verarbeitung. Erachtet man also nur aktive Handlungen als Entscheidungsbeitrag, die eine „conditio sine qua non"-Konditionalität für die Verarbeitung haben, würde in der Rechtssache Jehovan todistajat kein Beitrag der Glaubensgemeinschaft vorliegen.

Denkbar scheint also in Grenzen, dass bereits ein Gewährenlassen bzw. Unterlassen des Eingreifens als hinreichender Entscheidungsbeitrag zu verstehen ist. Denn solange ein gemeinsam Verantwortlicher einen Entscheidungsspielraum dahingehend hat, dass

---

[517] Dazu unten.

[518] Vgl. a. *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 41; *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 87 ff.

[519] Dabei ist diese Frage von der Problematik abzugrenzen, ob die reine Billigung von Zwecken und Mitteln ausreichend für eine gemeinsame Verantwortlichkeit ist, dazu: Kapitel 4 H. I. Die reine Billigung von Zwecken und Mitteln als gemeinsame Entscheidung?

[520] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 71.

er eingreifen oder gewähren lassen kann, besteht auch ein hinreichender Einfluss auf die Verarbeitung. Dies wird vor allem dann deutlich, wenn man die Verantwortlichkeit nicht nur als Entscheidungskompetenz, sondern korrespondierend hierzu auch als Kontrollkompetenz versteht.[521] Ähnlich formuliert auch der EDPS seine Anforderungen an die gemeinsame Entscheidung. So soll die Chance bzw. das Recht, die Zwecke und Mittel der Verarbeitung zu bestimmen, ausreichend sein.[522] Insgesamt sollte daher ein Unterlassen, sofern diesem im Rahmen eines Entscheidungsspielraums eine Entscheidungsqualität entnommen werden kann, hinreichend für einen Entscheidungsbeitrag sein. Das Erfordernis eines aktiven Beitrags wäre eine reine Förmelei, die zudem Umgehungskonstruktionen begünstigen könnte. Zudem würde die Wertung eines Unterlassens als Entscheidungsbeitrag auch Unsicherheiten hinsichtlich der Duldung eines Verhaltens umgehen. Zu denken wäre bei einem Entscheidungsbeitrag durch Unterlassen an das Gewährenlassen bei der Nutzung fremder Infrastruktur oder Daten, sowie ferner die Fälle eines „rogue processors", also eines Auftragsverarbeiters im Auftragsverarbeiterexzess.

VI. Rechtsprechung des EuGH

Vergleicht man die drei ersten Urteile des EuGH zur gemeinsamen Verantwortlichkeit, also in den Rechtssachen Wirtschaftsakademie, Jehovan todistajat und Fashion ID,[523] fällt auf, dass der EuGH in der Fashion ID erstmals betont, dass ein gemeinsam Verantwortlicher die Verarbeitung entscheidend beeinflusst.[524] Dabei zeigt sich eine Konkretisierung der Rechtsprechung von dem Beitrag und der Beteiligung in der Rechtssache Wirtschaftsakademie[525] über die Einflussnahme in Jehovan todistajat[526] zu

[521] Vgl. *Hacker*, MMR 2018, 779, 780.

[522] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 23; ebenso: *Cimina*, ERA Forum 2020, 7.

[523] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[524] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 78: „[...] entscheidend das Erheben und die Übermittlung [...] zugunsten des Anbieters [...] beeinflusst, die ohne [diese Handlung] nicht erfolgen würden."

[525] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36, 39: „Folglich trägt der Betreiber einer auf Facebook unterhaltenen Fanpage zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite bei.", „[...] durch die von ihm vorgenommene Parametrierung [...] an der Entscheidung über die Zwecke und Mittel der Verarbeitung [...] beteiligt ist."

[526] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 68: „[...] aus Eigeninteresse [...] Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt".

der entscheidenden Beeinflussung in Fashion ID.[527] Diese entscheidende Beeinflussung wird dann mit einer Mitwirkung an der Entscheidung über die Zwecke und Mittel gleichgesetzt.[528]

Auffällig ist dabei, dass – jedenfalls scheinbar – das Bezugsobjekt der Beteiligung, Einflussnahme bzw. Beeinflussung von der Entscheidung über die Zwecke und Mittel der Verarbeitung zur Verarbeitung als solcher wechselt. Dabei muss aber berücksichtigt werden, dass der Bezug zur Verarbeitung in der Rechtssache Fashion ID allein schon sprachlich bedingt war, da der EuGH am Satzende festhielt, dass die Verarbeitung ohne die Handlung des gemeinsam Verantwortlichen gar nicht stattgefunden hätte.[529] Ebenso hielt der EuGH in der folgenden Randnummer fest, dass die Verantwortlichen somit gemeinsam über die Mittel entschieden hätten.[530] Letztlich ist Bezugspunkt des Entscheidungsbeitrags, auch bei Erwähnung der Verarbeitung, also immer die Entscheidung über die Zwecke oder Mittel der Verarbeitung insgesamt. Dabei wird der EuGH in der Rechtssache Fashion ID hinsichtlich des Entscheidungsobjekts konkreter, da er nicht nur pauschal auf die Verarbeitung oder die Entscheidung über die Zwecke und Mittel verweist, sondern spezifisch auf die Entscheidung über die Mittel.[531] Sofern die entscheidende Beeinflussung der Entscheidung über die Mittel bereits für eine gemeinsame Verantwortlichkeit ausreicht, muss dies erst recht für die entscheidende Beeinflussung der Entscheidung über die Zwecke gelten.[532] Dies ergibt sich insbesondere daraus, dass die Zweckfestlegung im Rahmen der Zweckbindung gem. Art. 5 Abs. 1 lit. b DSGVO elementare Bedeutung für die Verarbeitung hat.[533] Objekt der entscheidenden Beeinflussung muss in jedem Fall eines der Objekte der Entscheidung sein, also entweder die Zwecke oder die Mittel. Für eine gemeinsame Entscheidung wiederum muss nach der Rechtsprechung des EuGH ein individueller Akteur also entweder die Entscheidung über die Zwecke oder Mittel entscheidend[534]

---

[527] Vgl. *Gierschmann*, ZD 2020, 69, 70 f.

[528] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 68; bestätigt in: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 68.

[529] A. das „im Übrigen" (in der englischen Version „moreover") ist stilistisch bedingt und gleichermaßen nicht als obiter dictum zu verstehen. Bei der entscheidenden Beeinflussung handelt es sich vielmehr um die ratio decidendi.

[530] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 79.

[531] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 78 f.

[532] Vgl. statt vieler die Annahme der Art. 29-Datenschutzgruppe, dass eine Entscheidung über die Zwecke der Verarbeitung immer eine Stellung als Verantwortlicher bedinge: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[533] Vgl. Art. 5 Abs. 1 lit. c - e DSGVO.

[534] Der Sprachwitz überlebt die Übersetzung ins Englische leider nicht, da die Definition hier „determine" verwendet, während das Urteil von „decisive" spricht.

beeinflussen. Insgesamt müssen die gemeinsam Verantwortlichen dann über alle Aspekte der Zwecke und Mittel entschieden haben.

1. Fashion ID

Was genau aber heißt entscheidend?[535] Sehr konkret wird der EuGH hierzu nicht. In der Rechtssache Fashion ID legte er den Schwerpunkt auf die Ermöglichung der Verarbeitung.[536] So scheint die Einbindung des Programmcodes des Social Plugins[537] in dem Wissen um die Ermöglichung der Verarbeitung ausreichend.[538] Dabei hatte der Websitebetreiber in der Rechtssache Fashion ID unter anderem eingewandt, er habe keinen Einfluss auf die vom Webbrowser des Besuchers an den Plattformbetreiber übermittelten Daten.[539] Diesen Einwand könnte man als fehlenden Einfluss auf die wesentlichen Elemente der Mittel der Verarbeitung, nämlich die verarbeiteten personenbezogenen Daten verstehen. Man kann die Ermöglichung der Verarbeitung als solche aber auch als Entscheidung über die wesentlichen Elemente der Mittel der Verarbeitung begreifen.[540] Der EuGH selbst setzt sich hiermit nicht weiter auseinander, sondern lässt die Ermöglichung der Datenerhebung gegenüber dem Plattformbetreiber bzw. die Übermittlung an diesen als gemeinsame Entscheidung über die Mittel genügen.[541] In diesem Sinne scheint also jedenfalls eine „conditio sine qua non"-Konditionalität ausreichend.[542]

Geht man weiter davon aus, dass sich die Rechtsprechungslinie des EuGH in der Rechtssache Fashion ID gegenüber den vorherigen Urteilen nicht fundamental geändert hat, kann man auch die Mitwirkungshandlungen der gemeinsam Verantwortlichen in den Rechtssachen Wirtschaftsakademie und Jehovan todistajat

[535] *Alsenoy*, CLSR[28] (2012), 25, 37; vgl. zur Komplexität der Kausalität von Handeln in einer zunehmend digitalisierten Welt: *Spiecker gen. Döhmann*, CR 2016, 698, 700 f.

[536] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 75 ff.; vgl. das ULD bereits 2011 *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 150.

[537] Zu weiteren Anwendungsfällen: *Kremer*, CR 2019, 676, Rn. 29 ff.

[538] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 77.

[539] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 34.

[540] Dazu: Kapitel 4 I. IV. Der Entscheidungsspielraum als Voraussetzung für einen Entscheidungsbeitrag. A.A. anscheinend: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 20. Der Verantwortliche räume anderen die Gelegenheit zur Datenverarbeitung ein, „ohne selbst damit befasst zu sein."

[541] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 75 ff. Im Tenor spricht der EuGH von Erhebung und Übermittlung (siehe a. ebd., Rn. 76). Auf welche Vorgänge er sich dabei bezieht, bleibt unklar und verwundert aufgrund der Abgrenzung einzelner Vorgänge in ebd., Rn. 70 ff. erheblich.

[542] *Golland*, K&R 2019, 533, 534.

für eine Bestimmung des vom EuGH verwendeten Begriffs „entscheidend" heranziehen.

2. Jehovan todistajat

Die Einflussnahme in der Rechtssache Jehovan todistajat bestand nach den Ausführungen des EuGH in der Ermunterung der verkündigenden Mitglieder, überhaupt Daten zu erheben.[543] Allerdings erschöpfte sich diese Einflussnahme nicht in einer Art „Anstiftung", sondern bestand auch darin, dass die Gemeinden die Verkündigungstätigkeit insgesamt – aber nicht konkret die Datenerhebung – organisierten und koordinierten. Zudem führten die Gemeinden Listen von Personen, die nicht mehr von den verkündigenden Mitgliedern aufgesucht werden wollten. Insgesamt war die Analyse des EuGH, durch die Angaben aus der Vorlage bedingt, nicht sehr spezifisch. Dies räumte der EuGH auch selbst ein.[544] Da der Fokus des EuGH in dieser Entscheidung auf dem gemeinsamen Zweck zu liegen scheint,[545] dürfte die Ermunterung zur Datenerhebung insgesamt, anhand der Organisation und Koordination der Gemeinden, maßgeblich gewesen sein. Demnach scheint bereits die lose Unterstützung der Verarbeitung von anderen gemeinsam Verantwortlichen im Rahmen eines gemeinsamen Zweckes hinreichend für eine entscheidende Beeinflussung.[546] Dabei könnte man die entscheidende Beeinflussung auch in der Bestimmung des gemeinsamen Zweckes sehen, den sich die verkündigenden Mitglieder zu-eigen-machen.[547] Über die Mittel scheinen die verkündigenden Mitglieder der Gemeinschaft hingegen selbst entschieden zu haben, wenn auch mit einer gewissen Hilfestellung der Gemeinschaft.

3. Wirtschaftsakademie

Die Beteiligung des Fanpage-Betreibers in der Rechtssache Wirtschaftsakademie an der Entscheidung über die Zwecke und Mittel bestand laut EuGH in der Parametrierung der Fanpage im Rahmen ihrer Einrichtung.[548] Der Fanpage-Betreiber konnte aufgrund der Parametrierung die Erstellung der anonymisierten Besucherstatistik seitens

[543] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 70 ff.; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 26 f.

[544] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 73: „[...] was jedoch das vorlegende Gericht anhand sämtlicher Umstände des vorliegenden Falles zu beurteilen hat."

[545] Dazu: Kapitel 4 F. III. Rechtsprechung des EuGH.

[546] Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 35.

[547] Vgl. EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 73.

[548] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36, 39.

Facebooks beeinflussen. Unabhängig davon, dass der Fanpage-Betreiber die hierzu verwendeten Daten nie selbst sah,[549] konnte er jedenfalls die Kategorien von betroffenen Personen anhand der Parametrierung bestimmen. Somit konnte er die Verarbeitung der Besucherstatistik zumindest in einem dem Verantwortlichen vorbehaltenen Kriterium i.S.v. Art. 28 Abs. 3 DSGVO bestimmen. Voraussetzung der Verarbeitung zur Besucherstatistik war die Erhebung der Daten der Fanpagebesucher durch das von dem Plattformbetreiber gesetzte Cookie.[550] Der Plattformbetreiber brauchte für die weitere Verarbeitung zur Besucherstatistik notwendigerweise diese Daten, unabhängig davon, dass er mit den erhobenen Daten gegebenenfalls noch andere, eigene Zwecke verfolgte.[551] Der Fanpage-Betreiber konnte hingegen seinen, laut EuGH maßgeblichen, Zweck der Besucherstatistik nicht ohne diesen Erhebungsvorgang erreichen.[552] Für den Fanpage-Betreiber bildeten also die Erhebung der Besucherdaten anhand des Cookies seitens des Plattformbetreibers sowie die Verarbeitung dieser Besucherdaten zur Besucherstatistik seitens des Plattformbetreibers eine Vorgangsreihe aufgrund des einheitlichen Zweckes.

Hinsichtlich dieser Vorgangsreihe leistete der Fanpage-Betreiber zwei Beiträge.[553] Zum einen war dies die Einrichtung der Fanpage, da ohne die Einrichtung der Fanpage der Plattformbetreiber nicht personenbezogene Daten über deren Besucher überhaupt hätte erheben können.[554] Dies galt abseits der der Plattform fremden Besuchern auch für die registrierten Nutzer der Plattform, da jedenfalls die Daten des konkreten Besuchs der Fanpage durch diese Nutzer nicht hätten erhoben werden können.[555] Zum anderen beeinflusste der Fanpage-Betreiber durch die Parametrierung der Fanpage die für die Besucherstatistik verwendeten Daten.[556] Separiert man diese Vorgangsreihe in die zwei individuellen Vorgänge, so wie sie sich aus der Perspektive des Plattformbetreibers darstellen, nämlich die Erhebung der Daten für die Verbesserung

[549] Was nach EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 38 ohnehin nicht erforderlich war.

[550] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 33 f.

[551] Sinnvollerweise konnte also der Fanpage-Betreiber a. nur für Verarbeitungsvorgänge von solchen personenbezogenen Daten gemeinsam verantwortlich sein, die für die Bereitstellung der Besucherstatistik notwendig waren.

[552] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34, 38.

[553] Vgl. a. BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 21; ähnlich wohl: *Wagner*, ZD 2018, 307, 309.

[554] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34, 38.

[555] Vgl. zum Begriff Nutzer: EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 35.

[556] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 36. *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 41 betonen, dass ohne die Parametrierung die Verarbeitung zur Besucherstatistik gar nicht stattgefunden hätte.

ihres eigenen Werbesystems[557] und, im Austausch für die Ermöglichung der Erhebung seitens der Fanpagebetreiber, die Erstellung der Besucherstatistik für diese, lassen sich die individuellen Beiträge des Fanpage-Betreibers dem entsprechenden Vorgang zuordnen. Folglich ist neben der reinen „conditio sine qua non"-Konditionalität der Ermöglichung einer Verarbeitung auch die Beeinflussung von wesentlichen Elementen der Mittel, die nur dem Verantwortlichen vorbehalten sind,[558] ausreichend im Sinne einer entscheidenden Beeinflussung.[559] Diese Beeinflussung der wesentlichen Elemente der Mittel wäre eben hinsichtlich der Parametrierung die Festlegung der Kategorien betroffener Personen i.S.v. Art. 28 Abs. 3 DSGVO.

Dass die Parametrierung der Fanpage allein nicht das entscheidende Kriterium für die Beteiligung des Fanpage-Betreibers an der gemeinsamen Entscheidung über Zwecke und Mittel der Verarbeitung war, ergab sich nicht zuletzt daraus, dass der EuGH dieses Kriterium für die Rechtssache Fashion ID, trotz eines sehr ähnlichen Sachverhalts, nicht mehr aufgegriffen hatte.[560] In der Rechtssache Fashion ID fanden sich im Sachverhalt keinerlei Ausführungen zu einer Parametrierung. Dies spricht dafür, bereits die Ermöglichung der Verarbeitung in der Rechtssache Wirtschaftsakademie als ausreichenden Entscheidungsbeitrag für die gemeinsame Entscheidung zu erachten.[561] Eine Parametrierung scheint, jedenfalls für die Einbindung des Social Plugins, entbehrlich. Dieses Ergebnis dürfte im Hinblick auf die praktische Anwendbarkeit der Definition des gemeinsam Verantwortlichen und eine Erheblichkeitsschwelle hierfür zu begrüßen sein.[562] Die Parametrierung der Fanpage in Wirtschaftsakademie lässt sich schließlich auch so verstehen, dass damit nur die Verantwortlichkeit des Fanpage-Betreibers für die weitere Verarbeitung zur Erstellung der Statistik begründet wurde.

---

[557] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 34.

[558] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23. *Kartheuser/Nabulsi*, MMR 2018, 717, 718 entnehmen diesen Ausführungen der Art. 29-Datenschutzgruppe einen bestimmenden Einfluss. Woraus sie dies ableiten, bleibt unklar. Denkbar wäre dies an der Entscheidung, die einen Verantwortlichen kennzeichnet, festzumachen.

[559] Ähnlich: *Hanloser*, ZD 2019, 455, 459.

[560] A. EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 41 macht deutlich, dass die Parametrierung nicht ausschlaggebend sein könne, da plattformexterne Nutzer keine entsprechenden Angaben bei der Plattform gemacht haben könnten.

[561] So wohl a.: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 21; *Golland*, ZD 2020, 397, 399; Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 123; eingeschränkt zustimmend: Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 29 ff. Der Plattformbetreiber hatte das Argument der Parametrierung noch angegriffen: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 13.

[562] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 45.

Das BVerwG hatte nach dem Urteil des EuGH in seiner Zurückverweisung der Entscheidung an das OVG Schleswig entschieden, dass der Begriff des gemeinsam Verantwortlichen so auszulegen sei, dass hierunter auch Stellen fallen sollten, die anderen die Gelegenheit der Datenverarbeitung einräumten, ohne selbst damit befasst zu sein.[563] Auch das BVerwG scheint folglich die Ermöglichung der Verarbeitung als ausreichend zu erachten.

4. Google Spain

Dass die Ermöglichung einer Verarbeitung als solche nicht der einzige Entscheidungsbeitrag ist, der die Erheblichkeitsschwelle für eine entscheidende Beeinflussung erreicht, deutete sich bereits in der Rechtssache Google Spain[564] an.[565] Hier hatte der EuGH im obiter dictum erwähnt, dass es zumindest denkbar erscheint, bereits das Unterlassen des Ausschlusses einer Website von der Indexierung durch einen Suchmaschinenbetreiber seitens des Websitebetreibers als ausreichenden Beitrag zu einer gemeinsamen Verantwortlichkeit anzusehen.[566] Allerdings hatte der EuGH diesen Ansatz nicht weiter vertieft, so dass die Aussagekraft dieser Erwägungen insoweit beschränkt bleibt.[567]

5. Kritik

Die extrem kasuistische Herangehensweise des EuGH bzw. die nicht erkennbare Systematik im Hinblick auf die Erheblichkeitsschwelle des Entscheidungsbeitrags eines gemeinsam Verantwortlichen führen notwendigerweise zu einer starken Rechtsunsicherheit. Eine „conditio sine qua non"-Konditionalität, also die Ermöglichung einer Verarbeitung überhaupt, stellt sicherlich einen äußerst gewichtigen Entscheidungsbeitrag zu einer Verarbeitung dar.[568] Gleichermaßen lässt sich, wie die Schlussanträge des Generalanwalts in der Rechtssache Fashion ID erkennen lassen, dieser Ansatz zur Bestimmung eines Entscheidungsbeitrags auch ad absurdum treiben.[569] Die Angreifbarkeit der Entscheidungen des EuGH zur gemeinsamen Verantwortlichkeit ergibt sich nicht zuletzt

[563] BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 20.
[564] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857.
[565] Spekulativ: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 66.
[566] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 40.
[567] Kritisch: *Spindler*, JZ[69] (2014), 981, 983.
[568] Vgl. etwa *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 50 f.
[569] Etwa der Beitrag des Stromversorgers zu einer Verarbeitung: EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 74.

auch aus der fehlenden systematischen Grundierung der Begriffe der Zwecke und Mittel (der Entscheidung).[570] Versteht man daher die Ermöglichung einer Verarbeitung als Entscheidung über die wesentlichen Elemente der Mittel, lässt sich ein Entscheidungsbeitrag bereits besser eingrenzen.

VII. Position der Aufsichtsbehörden

1. Art. 29-Datenschutzgruppe

Das WP 169 der Art. 29-Datenschutzgruppe zum Verantwortlichen ging dem Urteil in der Rechtssache Fashion ID fast zehn Jahre voraus. Ebenso wie die drei ersten Urteile des EuGH zur gemeinsamen Verantwortlichkeit erging es noch vor dem Hintergrund der DSRL. Nach der Art. 29-Datenschutzgruppe schien ein Entscheidungsbeitrag zu den Zwecken ausreichend für eine Einordnung als gemeinsam Verantwortlicher.[571] Daneben war ein Entscheidungsbeitrag zu den Mitteln nur dann maßgeblich, wenn er die wesentlichen Elemente[572] der Mittel betraf.[573] Ob dies auch in Ermangelung einer Auftragsverarbeitung gelten konnte, in der ja ein Auftragsverarbeiter über die unwesentlichen Elemente der Mittel hätte entscheiden können, bleibt unklar.[574] Zwar stellte das WP 169 selbst die Frage, wie detailliert jemand über die Zwecke und Mittel einer Verarbeitung entscheiden müsse, um als Verantwortlicher zu gelten,[575] insbesondere im Hinblick auf gemeinsam Verantwortliche und die Abgrenzung zum Auftragsverarbeiter. Allerdings wurde diese Frage letztlich nicht konkret beantwortet. Im Rahmen eines pragmatischen Ansatzes sollte größeres Gewicht auf die Ermessensfreiheit bei der Entscheidung über die Zwecke und auf den Spielraum bei der Entscheidungsfindung gelegt werden. Was dies genau bedeuten sollte, wurde nicht weiter erläutert.

Die Argumentation des EuGH zur entscheidenden Beeinflussung der Verarbeitung in der Rechtssache Fashion ID[576] zeigt gewisse Ähnlichkeiten zum WP 169. So könnte man die entscheidende Beeinflussung der Mittel als Entscheidung über die

[570] Kritisch a.: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 46.

[571] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[572] Dazu: Kapitel 2 D. Mittel.

[573] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23.

[574] Siehe a.: Kapitel 5 F. „Datenschutzrechtliche Beihilfe".

[575] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 16.

[576] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 78.

wesentlichen Elemente der Mittel verstehen. Ob der EuGH in der Rechtssache Fashion ID allerdings tatsächlich auf das WP 169 anspielte, bleibt mangels expliziter Bezugnahme unklar. Zudem passt auch das Bezugsobjekt der „entscheidenden Beeinflussung" bei penibler Anwendung der Ausführungen des WP 169 nicht. So bezieht sich die Entscheidung in dem WP 169 auf die wesentlichen Elemente der Mittel, in der Rechtssache Fashion ID hingegen beschreibt der EuGH die Beeinflussung der Verarbeitung selbst als entscheidend.

Bezüge zur späteren Rechtsprechung des EuGH finden sich aber auch in Beispiel 14[577] (Werbung auf Basis von Behavioural Targeting) des WP 169. Dieses Beispiel beschäftigte sich mit der Sammlung von Daten zur Bereitstellung von zielgerichteter Werbung an Internetnutzer. Dabei werden für die Auswahl der anzuzeigenden Werbeanzeigen, die von den Nutzern besuchten Websites und die von diesen durchgeführten Suchanfragen analysiert. Die Erhebung dieser Daten kann dabei, je nach vertraglicher Vereinbarung, sowohl durch die Anbieter von Online-Inhalten selbst als Teil der Vermarktung von Werbeflächen wie auch durch die Betreiber von Online-Werbenetzwerken erfolgen. Grundsätzlich ordnete die Art. 29-Datenschutzgruppe zwar sowohl den Anbieter von Online-Inhalten[578] wie auch den Betreiber des Online-Werbenetzwerks[579] als jeweils autonome Verantwortliche für ihre eigenen Zwecke und Mittel ein. Je nach Art der Zusammenarbeit zwischen dem Anbieter von Online-Inhalten und dem Betreiber des Online-Werbenetzwerks könne aber auch eine gemeinsame Verantwortlichkeit vorliegen. Dies sollte etwa dann vorliegen, wenn der Anbieter von Online-Inhalten personenbezogene Daten an den Betreiber des Online-Werbenetzwerks übermittelt, indem der Anbieter seine Besucher auf die Website des Betreibers umleitet.[580] Eine gemeinsame Verantwortlichkeit ergebe sich dabei aus dem gemeinsamen Zweck zielgerichteter Werbung anhand der dafür erforderlichen Verarbeitungsvorgänge als einheitliche Vorgangsreihe. Als Folge der gemeinsamen Verantwortlichkeit solle der Anbieter von Online-Inhalten dann unter anderem die betroffenen Personen über den Zugang des Betreibers des Online-Werbenetzwerks zu ihren Daten informieren und der Betreiber des Online-Werbenetzwerks solle die Erfüllung von Betroffenenrechten sicherstellen.

---

[577] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 28.

[578] Im Hinblick auf die notwendigen Informationen für die Darstellung der Inhalte wie Nutzerprofil, IP-Adresse, Standort, Sprache des Betriebssystems usw.

[579] Im Hinblick auf die Überwachung von Nutzern über mehrere Websites.

[580] Damit scheint aber nicht die Umleitung auf die Website insgesamt gemeint zu sein, sondern bereits die Einbindung von Webseitenelementen des Betreibers eines Online-Werbenetzwerks.

2. Europäischer Datenschutzbeauftragter (EDPS)

Der EDPS versteht in seinen, nach dem Urteil des EuGH in der Rechtssache Fashion ID veröffentlichten, Leitlinien zum Verantwortlichen explizit bereits das Eingehen in eine Vereinbarung mit mehreren Akteuren[581] als Grundlage für eine gemeinsame Verantwortlichkeit.[582] Im Rahmen dieses Eingehens in eine Vereinbarung müsse die Chance/das Recht bestehen, die Zwecke und wesentlichen Elemente der Mittel der Verarbeitung festzulegen. Dabei sei eine Kenntnis des allgemeinen oder groben Zweckes und der (wesentlichen Elemente der) Mittel nötig.

3. Europäischer Datenschutzausschuss (EDPB)

Die Leitlinien des EDPB verlangen zur Feststellung einer gemeinsamen Verantwortlichkeit, ähnlich wie bereits die Art. 29-Datenschutzgruppe,[583] eine Analyse des tatsächlichen Einflusses auf die Zwecke und Mittel der Verarbeitung.[584] Alle bestehenden oder vorgesehenen Vereinbarungen zwischen potenziellen gemeinsam Verantwortlichen sollten darauf überprüft werden, ob sie das tatsächliche Verhältnis der Akteure widerspiegeln. Demnach solle eine formelle Festlegung[585] der gemeinsamen Verantwortlichkeit nicht ausreichen, da sie oft nicht erfolge oder nicht notwendigerweise den Fakten[586] entspreche. Maßgeblich für die Beteiligung an der Entscheidung über Zwecke und Mittel sei ein entscheidender Einfluss darauf, ob und wie die Verarbeitung stattfinde.[587] Dies kann man prinzipiell so verstehen, dass ein Einfluss auf die Mittel (das „Ob" und „Wie") der Verarbeitung ausreiche. Da der EDPB aber insgesamt eine Entscheidung über die Zwecke und Mittel verlangt,[588] kann dies maximal die Erheblichkeitsschwelle für einen Entscheidungsbeitrag für die Mittel betreffen. Denn die verschiedenen Formen der gemeinsamen Entscheidung illustriert

[581] Der EDPS spricht dabei a. von „einigen".

[582] *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 23.

[583] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22 ff.

[584] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 52.

[585] Etwa per Vereinbarung oder Vertrag.

[586] Etwa weil der benannte „gemeinsam Verantwortliche" gar nicht in der Position ist über die Zwecke und Mittel zu entscheiden.

[587] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 30, 54.

[588] So scheinbar: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 36.

der EDPB mit der Möglichkeit einer „common decision" sowie einer „converging decision".[589]

VIII. Auslegungsansätze in der Literatur

Ähnlich diffus wie die Ausführungen des EuGH zu der Erheblichkeitsschwelle eines Entscheidungsbeitrags für die gemeinsame Entscheidung sind die Auslegungsansätze in der Literatur. *Martini* etwa verlangt eine „steuernde Einwirkung" auf die Verarbeitung.[590] Ein rein tatsächlicher Einfluss auf die Verarbeitung solle dafür ausreichen. Wie genau dieser steuernde Einfluss ausfallen soll, wird nicht weiter vertieft. Gerade das Verständnis dieses steuernden Einflusses wäre allerdings wichtig. Denn es scheint nur schwer vorstellbar, dass spätestens bei einer gemeinsamen Verantwortlichkeit von mehr als zwei Akteuren jeweils eine „steuernde Einwirkung" der Akteure vorliegt. Bei zwei Akteuren könnte zumindest eine „steuernde Einwirkung" auf die Zwecke einerseits und die Mittel andererseits vorliegen. Allerdings fordert *Martini* die „steuernde Einwirkung" eines individuellen gemeinsam Verantwortlichen sowohl auf die Zwecke wie auch Mittel der Verarbeitung. Versteht man die „steuernde Einwirkung" zudem nur als Möglichkeit der Einwirkung auf die Verarbeitung, stellt sich die Frage, wie diese Möglichkeit zu ermitteln wäre. Ein ähnlicher Ansatz findet sich auch bei *Hartung*, der eine wesentliche Entscheidungsbefugnis über Zwecke und Mittel voraussetzt, ohne dies näher zu konkretisieren.[591] Die wesentliche Entscheidungsbefugnis liege demnach entweder in der Entscheidung über die Zwecke und Mittel als solche oder in der maßgeblichen Beteiligung daran. *Hacker* wiederum fordert konkrete, signifikante Entscheidungsgewalt, allerdings ebenso ohne dies weiter zu vertiefen.[592]

Konkreter im Hinblick auf die Erheblichkeitsschwelle eines Entscheidungsbeitrags wird *Ingold*. Dieser bejaht die „Entscheidungshöhe" einer Mitentscheidung, wenn die Verarbeitung ohne den direktiven Input einer (der beteiligten) Stelle(n) potenziell andersartig gestaltet worden wäre.[593] Dabei soll nicht eine tatsächliche Mitwirkung an der Verarbeitung notwendig sein, eine Veranlassung oder direktive Mitgestaltung[594] ist bereits ausreichend. Dies ist ziemlich nahe an der bereits skizzierten Rechtsprechung des EuGH, der eine entscheidende Beeinflussung der Verarbeitung fordert. Eine

[589] Dazu: Kapitel 4 H. III. 4. c) Europäischer Datenschutzausschuss (EDPB).
[590] Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 19.
[591] Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 12.
[592] *Hacker*, MMR 2018, 779, 780.
[593] Sydow/Marsch/*Ingold*, Art. 26 DSGVO, Rn. 4.
[594] *Ingold* bezieht sich hier beispielhaft auf den Auftraggeber (als Pendant zum Auftragsverarbeiter).

weitere qualitative Einschränkung innerhalb der Entscheidungsobjekte der Zwecke und Mittel erfolgt bei *Ingold* nicht. Somit wären also auch Entscheidungsbeiträge, die dem Entscheidungsspielraum eines Auftragsverarbeiters entsprechen, allerdings nicht im Rahmen einer Weisungsgebundenheit erfolgen, ausreichend für einen Entscheidungsbeitrag. Im Hinblick auf den Wortlaut der Definition der gemeinsam Verantwortlichen ist dies nur konsequent. Der direktive Input muss aber so verstanden werden, dass andere gemeinsam Verantwortliche sich nicht ohne Weiteres über ihn hinwegsetzen können. Andernfalls wäre die Grenze zur Beratung eines Verantwortlichen, etwa durch einen Auftragsverarbeiter, kaum auszumachen.

Ähnlich positionieren sich *Specht-Riemenschneider/Schneider*, die einen adäquat-kausalen Beitrag zu einer Verarbeitung verlangen.[595] Wenn auch die Einschränkung über die Adäquanz, ähnlich wie sie bereits beim Generalanwalt in der Rechtssache Fashion ID anklang,[596] begrüßenswert ist, stellt sich die Frage, woher man die Voraussetzung einer Adäquanz im Rahmen der Definition des Verantwortlichen herleitet. Letztlich könnte man auch hier wiederum nur an die Rechtsprechung des EuGH in der Rechtssache Fashion ID und das Merkmal „entscheidend" anknüpfen. Rein sprachlich geht es bei „entscheidend" allerdings um eine Intensität oder Kausalität, nicht jedoch eine Adäquanz.

Kremer fordert die Möglichkeit der Beeinflussung der Zwecke oder Mittel der Verarbeitung durch einen gemeinsam Verantwortlichen.[597] Dabei könne auch die Veranlassung einer Verarbeitung ausreichen.[598] Eine gemeinsame Verantwortlichkeit soll dann nicht vorliegen, wenn ein Verantwortlicher zwar ursächlich bzw. mitwirkend an einer Verarbeitung beteiligt ist, es aber an einer gemeinsamen Willensbildung der Verantwortlichen fehle.[599] Dieses Szenario solle dann nur eine einfache Übermittlung darstellen. Wenn *Kremer* auch größtenteils zuzustimmen ist, scheint es schwer nachvollziehbar, warum die Ursächlichkeit oder Mitwirkung an einer Verarbeitung mangels gemeinsamer Willensbildung nicht zu einer gemeinsamen Verantwortlichkeit führen solle. Die Definition der gemeinsam Verantwortlichen spricht zwar von „gemeinsam entscheiden". Dies beinhaltet allerdings, wie bereits gezeigt, nicht zwangsläufig eine gemeinsame Willensbildung im Sinne eines prozessbezogenen

[595] *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 505.
[596] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 74.
[597] *Kremer*, CR 2019, 225, Rn. 15. Zusammenfassend: ebd., Rn. 17.
[598] Anscheinend ist also keine inhaltliche Beeinflussung unbedingt notwendig.
[599] *Kremer* spricht hier von einem Nebeneinander der Verarbeitung. Der Bezug auf *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24 scheint aber fehl am Platz, da die Art. 29-Datenschutzgruppe dort auf fehlende gemeinsame Zwecke oder Mittel abstellte.

Verständnisses der gemeinsamen Entscheidung. Vielmehr können für eine gemeinsame Entscheidung nach dem ergebnisbezogenen Verständnis auch kumulative Entscheidungsbeiträge ausreichen.[600] Insbesondere im Sachverhalt zu der Rechtssache Fashion ID ist nicht ersichtlich, inwiefern dort eine gemeinsame Willensbildung der gemeinsam Verantwortlichen vorliegen sollte, da es nach Bereitstellung des Social Plugins durch den Plattformbetreiber nicht zu einer weiteren Abstimmungsschleife mit dem Websitebetreiber kam.

Erkennbar ist in den aufgezeigten Auslegungsansätzen aus der Literatur häufig die Intention, eine Bagatellschwelle für den Entscheidungsbeitrag eines gemeinsam Verantwortlichen herzuleiten. Wo diese Schwelle dann genau verlaufen soll, bleibt aber vielfach unklar.[601] Folglich dreht sich die Frage, wann eine solche Bagatellschwelle über- bzw. unterschritten wird, regelmäßig im Kreis, da die Autoren entweder selbst keine Schwelle formulieren oder aber andere Bedingungen, etwa Entscheidungsbeiträge zu den Zwecken und Mitteln, für eine gemeinsame Entscheidung voraussetzen, die sich weder am Wortlaut der Definition noch in der Rechtsprechung des EuGH festmachen lassen. Das Problem, dass sich eine solche Erheblichkeitsschwelle kaum festmachen lässt, mag dem Umstand geschuldet sein, dass der EuGH schlicht keine Möglichkeit hat, die Beteiligungsform an einer Verarbeitung nur anhand von deren Intensität zu variieren. Aus diesem „one-size-fits-all"-Ansatz des EuGH hinsichtlich der Verantwortlichkeit folgt etwa der Einwand, bei der Einbindung des Social Plugins in der Rechtssache Fashion ID handele es sich nur um eine „datenschutzrechtliche Beihilfe".[602] Nach den Verantwortlichkeitsrollen der DSGVO ist ein Akteur aber entweder Verantwortlicher, Auftragsverarbeiter oder eben ein datenschutzrechtliches Nullum. Im Hinblick auf die Möglichkeit weiterer Rechtsfortbildung durch den EuGH würde diesen eine vorschnelle Eingrenzung der Voraussetzungen einer gemeinsamen Verantwortlichkeit möglicherweise, ohne Not, für die Zukunft einschränken.[603] Dennoch wäre hinsichtlich der gemeinsamen Entscheidung abseits einer systematischen Ausdifferenzierung der Definition durch den Unionsgesetzgeber wenigstens eine Typologie durch die Rechtsprechung wünschenswert.

[600] Dazu: Kapitel 4 H. III. Inhalt des individuellen Entscheidungsbeitrags bei der gemeinsamen Entscheidung.

[601] *Hense*, DSB[44] (2020), 236, 236.

[602] Vgl. zum Begriff *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 175 ff. Kritisch hierzu: *Monreal*, CR 2019, 797, Rn. 34.

[603] Vgl. zur Flexibilität der Definition Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 49.

IX. Fazit

Sinnvoll erscheint für die Erheblichkeitsschwelle eines Entscheidungsbeitrags demnach insgesamt eine, wenn auch eingeschränkte, Rückbesinnung auf den Wortlaut der DSGVO. Der für einen individuellen gemeinsam Verantwortlichen hinreichende Entscheidungsbeitrag liegt demnach dann vor, wenn dieser zu den Zwecken **oder** aber den Mitteln einer Verarbeitung erfolgt. Hinsichtlich des jeweils anderen Entscheidungsobjekts reicht im Weiteren eine Billigung aus. Liegt in einem Verarbeitungsszenario zusätzlich auch noch eine Auftragsverarbeitung durch einen weiteren Akteur vor, muss, sofern alle unwesentlichen Elemente der Mittel durch den Auftragsverarbeiter vorgegeben werden, der Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen zu den Mitteln der Verarbeitung die wesentlichen Elemente dieser Mittel betreffen. Allgemein muss ein Entscheidungsbeitrag daneben einen zumindest binären Entscheidungsspielraum aufweisen und kann auch im Rahmen eines Unterlassens erfolgen. Er muss aber eine Konsequenz für die Verarbeitung jedenfalls insoweit haben, dass die Verarbeitung ohne diesen Entscheidungsbeitrag anders ausgefallen wäre.

J. Indizien für eine Abgrenzung zum Auftragsverarbeiter

Neben den erörterten Voraussetzungen eines Auftragsverarbeiters[604] bieten sich noch verschiedene Indizien für eine Analyse an, ob eine Auftragsverarbeitung oder aber gemeinsame Verantwortlichkeit vorliegt. Solche Indizien sind etwa eine formelle Übereinkunft zwischen den Akteuren, die Art der Interaktion und die Art der erbrachten Dienstleistung.[605] Ebenso sollte aber auch vorab geprüft werden, ob nicht eine reine Übermittlung zwischen singulären Verantwortlichen vorliegt.[606]

I. Formelle Übereinkünfte und allgemeines Auftreten der Akteure

Ein Indiz für eine Abgrenzung zwischen Auftragsverarbeitung und gemeinsamer Verantwortlichkeit kann zunächst sein, welche Art von formeller Übereinkunft die Akteure untereinander treffen. So ist nach Art. 26 Abs. 1 S. 2 DSGVO grundsätzlich eine

[604] Kapitel 2 G. Der Auftragsverarbeiter als Abgrenzungsobjekt.
[605] Siehe a. die Checkliste bei: *Gierschmann*, ZD 2020, 69, 72.
[606] *Kremer*, CR 2019, 225, Rn. 10.

Vereinbarung zwischen gemeinsam Verantwortlichen erforderlich. In dieser wird festgehalten, wer für welche Pflichten, sofern delegierbar,[607] aus der DSGVO zuständig ist.[608] Diese Vereinbarung kann aufgrund von unions- oder mitgliedstaatlichem Recht allerdings auch teilweise oder vollständig entfallen. Auftraggeber und Auftragsverarbeiter müssen hingegen grundsätzlich einen Vertrag gem. Art. 28 Abs. 3 DSGVO abschließen. Dieser zeichnet sich gegenüber der Vereinbarung aus Art. 26 Abs. 1 S. 2 DSGVO durch deutlich spezifischere Vorgaben aus. Auch dieser Vertrag kann durch ein anderes Rechtsinstrument auf unions- oder mitgliedstaatlicher Grundlage ersetzt werden.

Aufgrund der unterschiedlichen gesetzlichen Anforderungen an Vereinbarung und Vertrag sowie der damit einhergehenden Bezeichnung der Akteure erscheint dieses Indiz zunächst zur Abgrenzung von Auftragsverarbeitung und gemeinsamer Verantwortlichkeit gut geeignet. Dabei ist allerdings zu bedenken, dass es sich bei diesen formellen Übereinkünften nur um eine Selbstzuschreibung der Akteure handelt.[609] Dieser Charakter einer Selbstzuschreibung wird durch den Transparenzappell aus Art. 26 Abs. 2 S. 1 DSGVO deutlich. Die Vereinbarung soll zwar, muss aber keineswegs die tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen abbilden. Zudem setzt eine Abgrenzung anhand des Indizes einer formellen Übereinkunft voraus, dass eine solche überhaupt existiert. Die Vereinbarung zwischen gemeinsam Verantwortlichen und der Vertrag zwischen Auftraggeber und Auftragnehmer sind allerdings jeweils Folge einer tatsächlichen gemeinsamen Verantwortlichkeit bzw. Auftragsverarbeitung, nicht konstitutive Voraussetzung dafür. Die jeweilige Übereinkunft setzt also voraus, dass sich die Akteure ihrer datenschutzrechtlichen Rolle selbst bewusst sind. Insofern hat die formelle Übereinkunft für die beteiligten Akteure sowie Dritte nur eine geringe Indizwirkung.[610] Entscheidend bleiben vielmehr die tatsächlichen Funktionen und Beziehungen der Akteure. Deutlich wird hierbei auch, dass die früher zum BDSG a.F. vertretene Vertragstheorie, die einen Vertrag für die Auftragsverarbeitung als konstitutive Voraussetzung verlangte, hinfällig ist.[611]

---

[607] Dazu: Kapitel 4 L. V. Delegation von Pflichten zwischen gemeinsam Verantwortlichen.

[608] Insb. für Informationspflichten und Betroffenenrechte.

[609] Kühling/Buchner/*Hartung*, Art. 28 DS-GVO, Rn. 61; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 38; Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 20; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 15.

[610] Vgl. *Kremer*, CR 2019, 225, Rn. 9, 18; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22 f. *Schreiber*, ZD 2019, 55, 58 sieht ein Wechselspiel zwischen formeller Übereinkunft und tatsächlichen Gegebenheiten.

[611] *Kremer*, CR 2019, 225, Rn. 9 m.w.N.

Wie bereits die Art. 29-Datenschutzgruppe, weist auch der EDPB darauf hin, dass die Tatsache, dass ein Auftragsverarbeiter standardisierte Auftragsverarbeitungsverträge in Verhandlungen einbringt, nicht notwendigerweise zu einer Entscheidung des Auftragsverarbeiters selbst über die wesentlichen Aspekte[612] der Verarbeitung führe.[613] Denn der Auftraggeber als Verantwortlicher müsse diese standardisierten Auftragsverarbeitungsverträge ja nicht annehmen. Folglich bedinge die Erstellung des Auftragsverarbeitungsvertrag durch einen Auftragsverarbeiter nicht notwendigerweise seine Einordnung als Verantwortlicher.[614] Der Auftraggeber könne sich andererseits aber nicht wegen Datenschutzverstößen auf die Erstellung der Vertragsbedingungen durch den Auftragsverarbeiter berufen.[615] Der Auftraggeber müsse bei Bedarf Änderungen am Vertrag vornehmen können und der Auftragsverarbeiter könne auch nicht eigenmächtig die wesentlichen Elemente der Mittel ohne Zustimmung des Verantwortlichen ändern.[616] Die reine Verhandlungsposition eines Akteurs hinsichtlich der Verarbeitung impliziert also nicht notwendigerweise eine bestimmte datenschutzrechtliche Rolle.[617]

Dass formelle Übereinkünfte keine verbindliche Wirkung für die tatsächliche datenschutzrechtliche Rolle eines Akteurs haben sollen, illustrierte die Art. 29-Datenschutzgruppe in WP 169 mit dem Beispiel 6 (Personalvermittler).[618] In diesem Beispiel wird Unternehmen E durch Unternehmen H bei der Einstellung neuer Mitarbeiter unterstützt. Nach dem Vertrag soll H Auftragsverarbeiter sein und E Verantwortlicher. Gegenüber den Arbeitssuchenden tritt H allerdings als Verantwortlicher auf. Zusätzlich bietet H noch einen Mehrwertdienst an, indem er neben den bei E direkt eingegangen Bewerbungen auch noch seine eigene Datenbank nach Kandidaten durchsucht.[619]

---

[612] Gemeint sind damit wohl die Zwecke sowie die wesentlichen Elemente der Mittel.

[613] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 32 Fn. 18. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 30, 84, 108 ff. mit Beispielen in Rn. 30, 84 (Standardised cloud storage service bzw. Cloud service provider).

[614] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 110.

[615] Dazu: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 32 Beispiel 18 (E-Mail-Plattformen); *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 110.

[616] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 110. So sei etwa die Publikation der Änderungen des Auftragsverarbeitungsvertrags auf der Website des Auftragsverarbeiters nicht mit Art. 28 DSGVO vereinbar.

[617] Vgl. *Alsenoy*, CLSR[28] (2012), 25, 33.

[618] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 23.

[619] Der Sachverhalt des Beispiels wirkt dabei etwas wirr. Es wird nicht klar, wieso H für die Arbeitssuchenden als Verantwortlicher auftritt, gleichzeitig allerdings Bewerbungen direkt bei E eingehen. Während

Bei H soll es sich nach Ansicht der Art. 29-Datenschutzgruppe, entgegen der vertraglichen Vereinbarungen, um einen Verantwortlichen handeln. Zudem bestehe aufgrund der Personalvermittlung für E auch eine gemeinsame Verantwortlichkeit mit E.[620] Eine genaue Begründung liefert die Art. 29-Datenschutzgruppe nicht. Die Verantwortlichkeit von H dürfte sich hier daraus ergeben, dass H über wesentliche Elemente der Mittel, nämlich die zu verwendenden Daten, selbst entscheidet. Damit verlässt H den Entscheidungsspielraum eines Auftragsverarbeiters.[621] Der Auftraggeber E kann offensichtlich nicht über die beim Personalvermittler H verfügbaren Daten entscheiden, die nicht im Rahmen der Auftragsverarbeitung erhoben wurden. Denkbar wäre daneben, dass der Personalvermittler H auch über eigene Zwecke der für die Personalvermittlung erhobenen Daten (mit-)bestimmt, falls die gescheiterten Bewerbungen in die eigene Datenbank aufgenommen werden. Grundsätzlich wären die Daten gem. Art. 17 Abs. 1 lit. a DSGVO nach Beendigung der Verarbeitung, also der Personalvermittlung, zu löschen. Die gemeinsame Verantwortlichkeit dürfte sich aus der zumindest impliziten Billigung der Verwendung der eigenen Datenbank von H seitens E ergeben. Denn durch die zusätzlichen Daten des Personalvermittlers H ergibt sich insgesamt ein neuer Datensatz für die Personalvermittlung. Insofern bestehen gemeinsame Mittel. Deutlich wird anhand dieses Beispiels jedenfalls die begrenzte Indizwirkung von formellen Übereinkünften für eine Abgrenzung. Gleiches lässt sich auch dem Beispiel von SWIFT in WP 169 entnehmen.[622] Die reine Benennung als Auftragsverarbeiter im Vertrag führte noch nicht zu einer tatsächlichen Rolle als Auftragsverarbeiter.

Neben den formellen Übereinkünften im Speziellen wäre es aber auch denkbar, an das Auftreten der Akteure allgemein als Indiz anzuknüpfen,[623] etwa die Benennung der Verantwortlichen im Rahmen der Informationspflicht nach Art. 13 Abs. 1 lit. a DSGVO. Denkbar sind im Rahmen der gemeinsamen Verantwortlichkeit zwei Szenarien, in denen Auftreten und tatsächliche Rolle auseinanderfallen. So könnte ein gemeinsam Verantwortlicher wie ein Auftragsverarbeiter auftreten, obwohl er, mangels Weisungsgebundenheit, nicht die Voraussetzungen dafür erfüllt. Daneben könnte ein

E also vermutlich Stellen ausgeschrieben hat, sucht H parallel für E geeignete Kandidaten, ohne aber ein Tätigwerden für E offenzulegen.

[620] Vgl. a. das Beispiel von Lettershop-Dienstleistungen bei *Kremer*, CR 2019, 225, Rn. 53 ff.; ebenso: *Reif*, RdV 2019, 30, 31.

[621] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17; vgl. G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40.

[622] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[623] So etwa: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 34.

Auftragsverarbeiter den Eindruck erwecken, er wäre (gemeinsam) Verantwortlicher, obwohl er sich im Rahmen der Weisungen des Auftraggebers bewegt. Möglicherweise will dabei ein Verantwortlicher einen Auftragsverarbeiter nicht zu erkennen geben oder umgekehrt der Auftragsverarbeiter nicht den Verantwortlichen. Fraglich ist in diesen Szenarien, ob ein Auseinanderfallen von Auftreten und tatsächlicher Rolle Rückwirkungen auf diese Rolle hat.[624] Wie bereits dargestellt, sind nach den Definitionen des Verantwortlichen und Auftragsverarbeiters ausschließlich die tatsächlichen Verhältnisse entscheidend. Maßgeblich ist also allein die (gemeinsame) Entscheidung über Zwecke und Mittel der Verarbeitung.[625] Ein Anscheins-Verantwortlicher wird von der DSGVO nicht erfasst. Auch das allgemeine Auftreten ist als Indiz für eine Abgrenzung also nur beschränkt brauchbar.

Insgesamt sind also Selbstzuschreibungen in Übereinkünften oder das allgemeine Auftreten hinsichtlich der Rolle eines Akteurs nur ein geringes Indiz für dessen tatsächliche Rolle. Denkbar ist es hingegen, das Auftreten eines Akteurs im Rahmen von Schadensersatz, aufsichtsbehördlichen Maßnahmen sowie Geldbußen zu berücksichtigen. Bei gemeinsam Verantwortlichen kann im Rahmen der Aufteilung der Pflichten nach Art. 26 Abs. 1 S. 2 DSGVO zudem nur einer der Verantwortlichen gegenüber den betroffenen Personen auftreten. Allerdings muss dann über die anderen gemeinsam Verantwortlichen gem. Art. 13 Abs. 1 lit. a DSGVO informiert werden. Prinzipiell ist es nicht ausgeschlossen, dass unabhängig von der tatsächlichen Rolle eines Akteurs gegen Informations- und Transparenzpflichten verstoßen wird. Dies ergibt sich daraus, dass das Definitionselement des „Entscheidens“ keine rechtmäßige Entscheidung voraussetzt.[626] So könnte ein Auftragsverarbeiter unter Verstoß gegen die Informationspflicht als Verantwortlicher auftreten, mangels Entscheidung über die Zwecke und Mittel wäre er allerdings keiner. Umgekehrt kann der Auftragsverarbeiter auch durchaus unerkannt bleiben, da bezüglich der Auftragsverarbeitung keine Informationspflicht besteht.[627]

---

[624] Unklar: G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 38, 40.

[625] So a.: *Lezzi/Oberlin*, ZD 2018, 398, 400; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 38.

[626] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 11.

[627] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 34 Beispiel 20; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40.

II. Art der Interaktion

Die Art der Interaktion der Akteure,[628] also etwa ein Entscheiden miteinander und nicht bloß nacheinander,[629] ist als Indiz für eine Abgrenzung weitgehend ungeeignet. Dies ergibt sich vor allem aus der Rechtsprechung des EuGH sowie der hier vertretenen Auffassung, dass die gemeinsame Entscheidung ergebnisbezogen zu verstehen ist. Demnach reicht für eine gemeinsame Verantwortlichkeit auch ein Entscheiden nacheinander. Ein sinnvolles Indiz zur Abgrenzung zum Auftragsverarbeiter lässt sich dann anhand der Gegenpole miteinander und nacheinander nicht ableiten. Würde man ein Entscheiden miteinander, also ein prozessbezogenes Verständnis der gemeinsamen Entscheidung voraussetzen, hätte der Sachverhalt in der Rechtssache Fashion ID[630] als Auftragsverarbeitung bewertet werden müssen. Zwar lag in der Rechtssache Fashion ID nicht eine rein faktische, also möglicherweise zufällige, Zusammenarbeit vor,[631] gleichermaßen erfolgte aber auch keine gleichzeitige Einbeziehung der jeweils anderen Partei. Eine gemeinsame Verantwortlichkeit setzt zudem auch keine Bereitschaft der beteiligten Akteure voraus, eine gemeinsame Entscheidung im Sinne eines gemeinsamen Entscheidungsprozesses zuzulassen.[632] Nur die Billigung eines fremden Entscheidungsbeitrags ist nötig,[633] auch bei einer gemeinsamen Entscheidung nacheinander.

Abseits eines gemeinsamen Entscheidungsprozesses lässt sich eine hierarchische Aufteilung der Entscheidungsmacht über die Verarbeitung durchaus als Indiz für eine Abgrenzung zwischen einem gemeinsam Verantwortlichen und einem Auftragsverarbeiter heranziehen.[634] Allerdings auch nur insoweit, dass ein echtes Weisungsrecht des Verantwortlichen gegenüber dem vermeintlichen Auftragsverarbeiter besteht und nicht nur eine entsprechende Verhandlungsposition. Entscheidend wäre dann aber wiederum das Weisungsrecht und nicht die Art der Zusammenarbeit.

III. Art der Dienstleistung

Der EDPB weist darauf hin, dass die Rolle als Auftragsverarbeiter nicht von der Art bzw. Natur eines Akteurs abhängt, sondern von den konkreten Tätigkeiten in einem

---

[628] Dazu: Kapitel 4 H. III. 7. Antizipierte Entscheidungsbeiträge?
[629] Vgl. Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 9.
[630] Dazu: Kapitel 4 B. III. Fashion ID.
[631] Zum Begriff: Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 9.
[632] Anders: Auernhammer, 6. Auflage/*Thomale*, Art. 26 DSGVO, Rn. 9.
[633] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.
[634] *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 504; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 40.

spezifischen Kontext.[635] Demnach sei die Art der Dienstleistung eines Akteurs entscheidend dafür, ob er personenbezogene Daten im Auftrag eines Verantwortlichen verarbeite. So soll ein Akteur vor allem dann nicht Auftragsverarbeiter sein, wenn seine Dienstleistung nicht besonders auf die Verarbeitung personenbezogener Daten ausgerichtet ist oder die Verarbeitung nicht ein Kernelement der Dienstleistung darstellt.[636] Denn dann sei der Akteur häufig in der Lage, selbst die Zwecke und Mittel der Verarbeitung, die für die Erbringung der Dienstleistung notwendig sind, festzulegen. In dieser Situation sei der Akteur als Verantwortlicher und nicht als Auftragsverarbeiter anzusehen. Diese Annahme sei allerdings auch nicht zwingend und hänge vom Ausmaß der Kontrolle des Auftraggebers über die Verarbeitung durch den Dienstleister ab.[637] In jedem Fall sei eine Analyse des Einzelfalls notwendig. Die Art der Dienstleistung kann daher als, wenn auch schwaches, Indiz für eine Abgrenzung zwischen Auftragsverarbeiter und gemeinsam Verantwortlichen herangezogen werden. Maßgeblich für die tatsächliche Abgrenzung bleibt allerdings wiederum die Frage der Weisungsgebundenheit.

IV. Fazit

Die Abgrenzung zwischen Auftragsverarbeiter und gemeinsam Verantwortlichen muss, wie deutlich wurde, immer entlang der Voraussetzung der Weisungsgebundenheit des Auftragsverarbeiters erfolgen. Dabei sind allerdings auch Entscheidungsspielräume des Auftragsverarbeiters zu beachten. Sinnvolle Indizien für eine Weisungsgebundenheit können die Art der Dienstleistung sowie ein potenzielles Eigeninteresse des vermeintlichen Auftragsverarbeiters sein. Auch die Art. 29-Datenschutzgruppe schlug vor, anhand der Ausführlichkeit der von einem Verantwortlichen erteilten Weisungen, die den Handlungsspielraum eines Auftragsverarbeiters bestimmen, zu analysieren, ob ein Akteur ein Auftragsverarbeiter ist.[638] Daneben soll der Grad der Überwachung

[635] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 82.

[636] Der EDPB verwendet hier das Beispiel eines Taxi-Vermittlungsservices, der die Namen von Angestellten oder Gästen eines Unternehmens zum Zweck des Transports dieser verarbeitet. Vgl. a. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 40 Beispiel 3 Buchhaltung.

[637] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 83.

[638] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 34.

durch einen Verantwortlichen als Kriterium für das Vorliegen einer Auftragsverarbeitung dienen.[639] Eine permanente, sorgfältige Überwachung einer Verarbeitung deute demnach auf eine Auftragsverarbeitung hin.

K. Auftragsverarbeiterexzess und Mitarbeiterexzess

I. Grundlagen des Auftragsverarbeiterexzesses

Einen Sonderfall der Abgrenzung zum Auftragsverarbeiter stellt der Auftragsverarbeiterexzess dar. Dieser war im Rahmen der DSRL noch nicht normiert,[640] ist nun aber in Art. 28 Abs. 10 DSGVO explizit geregelt. Beim Auftragsverarbeiterexzess liegen die grundsätzlichen Voraussetzungen einer Auftragsverarbeitung, insbesondere die Bindung des Auftragsverarbeiters durch einen Vertrag oder ein anderes Rechtsinstrument, vor. Der Auftragsverarbeiter wäre gem. Art. 28 Abs. 3 lit. a DSGVO unter anderem gesetzlich gehalten sich innerhalb des durch die Weisungen vorgegebenen Rahmens[641] zu halten. Er entscheidet sich allerdings dennoch dazu, selbst die Zwecke und Mittel der Verarbeitung zu bestimmen.[642] Bei dieser Entscheidung überschreitet der Auftragsverarbeiters hinsichtlich der Mittel zumindest den Entscheidungsspielraum, welcher ihm zusteht.[643] Mit der Entscheidung über Zwecke und[644] (wesentliche Elemente der) Mittel nimmt der Auftragsverarbeiter bereits nach Art. 4 Nr. 7 DSGVO definitionsgemäß die Rolle eines Verantwortlichen ein. Insofern hat Art. 28 Abs. 10 DSGVO eigentlich lediglich deklaratorischen Charakter.[645] Ob sich der Auftragsverarbeiter sei-

[639] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 34.

[640] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18.

[641] Sydow/Marsch/*Ingold*, Art. 29 DSGVO, Rn. 1 spricht im Hinblick auf Art. 29 DSGVO von einem „Verarbeitungsverbot mit Weisungsvorbehalt".

[642] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 81.

[643] Dazu: Kapitel 2 G. III. Entscheidungsautonomie über die Mittel?

[644] Sinnvollerweise müsste es hier „oder" heißen, da ohnehin ein Szenario mit mehreren Akteuren vorliegt. Der Auftragsverarbeiter muss im Gegensatz zur Definition des singulären Verantwortlichen nicht über alles entscheiden. Aufgrund des Entscheidungsspielraums des Auftragsverarbeiter hinsichtlich der technischen und organisatorischen Maßnahmen würde diese Berücksichtigung allerdings die Norm sprachlich sehr komplex machen. Abseits dessen böte sich eine Definition oder jedenfalls normativ offensichtliche Differenzierung zwischen wesentlichen und unwesentlichen Elementen der Mittel an, so wie sie die Art. 29- Datenschutzgruppe vornimmt. A.A.: Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 16.

[645] Siehe a.: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and

nes Exzesses bewusst ist, ist irrelevant. Denn sowohl die Definition des Verantwortlichen als auch die des Auftragsverarbeiterexzesses verlangen nur die tatsächliche Entscheidung über Zwecke und Mittel der Verarbeitung.[646] Abgesehen von den Vorschriften zur Haftung, den Geldbußen und sonstigen Sanktionen, die zusätzlich für den Auftraggeber als Verantwortlichen weiter gelten, wird der ursprüngliche Auftragsverarbeiter ebenso wie ein Verantwortlicher behandelt. Dies beinhaltet alle damit verbundenen Pflichten. Liegt aufgrund eines Auftragsverarbeiterexzesses eine gemeinsame Verantwortlichkeit vor, bedingt dies zudem, dass eine eigene Rechtfertigung für die Verarbeitung vorliegen muss.[647] Denn diese kann beim Auftragsverarbeiterexzess nicht mehr vom Auftraggeber abgeleitet werden.

Den Auftragsverarbeiterexzess illustrierte die Art. 29-Datenschutzgruppe anhand von Beispiel 3[648] des WP 169. Dort erhält der vermeintliche Auftragsverarbeiter M von dem Verantwortlichen G personenbezogene Daten in Form einer Kundendatenbank zum Zwecke spezifischer Werbemaßnahmen. M will diese Kundendatenbank von G allerdings auch für die Werbemaßnahmen anderer Kunden einsetzen. Nach Ansicht der Art. 29-Datenschutzgruppe wird M durch dieses Hinzufügen eigener Zwecke zu den Zwecken der Verarbeitung, für die G die Kundendatenbank übermittelt hat, zu einem Verantwortlichen. Sinnvollerweise muss dieses Beispiel so verstanden werden, dass sobald der vermeintliche Auftragsverarbeiter aus der vertraglich vereinbarten Auftragsverarbeitung „ausbricht", indem er die Daten von G mit den Daten anderer Kunden vermischt oder nach Beendigung der Auftragsverarbeitung für G diese Daten nicht löscht, sondern weiterspeichert, er aufgrund eigener Zwecke für diese Verarbeitungen zum Verantwortlichen wird. Die reine Absicht, zum Zeitpunkt der Übermittlung bereits Zwecke jenseits der Auftragsverarbeitung verfolgen zu wollen, kann noch keine eigene Verantwortlichkeit des vermeintlichen Auftragsverarbeiters begründen.[649] Möglicherweise ist dieses Beispiel der Art. 29-Datenschutzgruppe aber auch einfach ungeschickt formuliert.[650]

---

processor in the GDPR, 07.07.2021, Rn. 36. Vgl. zur Übertragung von Art. 28 Abs. 10 DSGVO auf den Mitarbeiterexzess *Ambrock*, ZD 2020, 492, 494.

[646] So a.: Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 25.

[647] Vgl. EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 97 zu gemeinsam Verantwortlichen.

[648] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 18. Fast identisch der EDPB: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 81 Beispiel.

[649] Ganz abgesehen davon, dass dies a. nicht sinnvoll nachweisbar sein wird.

[650] Der vorangehende Absatz legt nahe, dass es um die Verantwortlichkeit für eine eigene Verarbeitung geht, nicht für die Übermittlung der Daten durch den Auftraggeber.

Der EuGH hat bislang nur zu der Frage, wie weit die Haftung des Auftraggebers bzw. Verantwortlichen im Falle eine Auftragsverarbeiterexzess reicht, entschieden. Laut Urteil in der Rechtssache NZÖG[651] solle die Haftung dann entfallen, wenn der Auftragsverarbeiter personenbezogene Daten für eigene Zwecke verarbeitet hat oder diese Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte.[652]

II. Gemeinsame Verantwortlichkeit als Folge des Auftragsverarbeiterexzesses

Ausgehend vom Wortlaut von Art. 28 Abs. 10 DSGVO wird der vermeintliche Auftragsverarbeiter durch den Auftragsverarbeiterexzess zunächst nur zum Verantwortlichen. Ob beim Auftragsverarbeiterexzess notwendigerweise immer eine gemeinsame Verantwortlichkeit zwischen Auftraggeber und ursprünglichem Auftragsverarbeiter besteht, scheint daher eher zweifelhaft.[653] Denkbar ist dies jedenfalls dann, wenn der Auftraggeber sich entweder den eigenen Entscheidungsbeitrag des ursprünglichen Auftragsverarbeiters zu eigen macht oder diesen explizit billigt, etwa indem er ihn genehmigt oder toleriert.[654] Ebenso wäre eine gemeinsame Verantwortlichkeit auch dann anzunehmen, wenn der Auftraggeber das Verhalten des ursprünglichen Auftragsverarbeiters hätte verhindern können. Wenn der Auftraggeber also das Verhalten des ursprünglichen Auftragsverarbeiters trotz Möglichkeit hierzu nicht unterbindet, entweder im Hinblick auf die Ermöglichung des Handelns oder mangels Erkennens des Verhaltens.[655] Diese implizite Billigung durch die fehlende Unterbindung muss nicht notwendigerweise eine aktive Handlung des Auftraggebers voraussetzen. Ausreichend wäre bereits das Untätigbleiben. Neben dem Hinzufügen eigener Zwecke durch den ursprünglichen Auftragsverarbeiter liegt auch dann eine gemeinsame Verantwortlichkeit mit dem Auftraggeber vor, wenn der Auftragsverarbeiter nicht nur Empfehlungen

[651] Dazu: Kapitel 4 B. IV. NZÖG (Nacionalinis visuomenes sveikatos centras).

[652] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 85

[653] So Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 24 zur fehlerhaften Auftragsverarbeitung. Kritisch: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 67. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 17 geht hier nur von der Möglichkeit aus.

[654] Dazu: Kapitel 4 G. Die Billigung fremder Zwecke oder Mittel als Teil der Entscheidung.

[655] Ähnlich *Ambrock*, ZD 2020, 492, 493, der stark von der Duldungsvollmacht abgrenzt. Maßgeblich ist demnach nicht der Rechtsschein, sondern die Kontrollmöglichkeit des Verantwortlichen.

bezüglich der dem Verantwortlichen (gesetzlich) vorbehaltenen Entscheidungen ausspricht, sondern diese direkt umsetzt.[656] Nutzen der Auftragsverarbeiter, insbesondere aber die dem Verantwortlichen unterstellten Personen[657] verarbeitete Daten für private Zwecke, ist eine gemeinsame Verantwortlichkeit schwer vorstellbar.[658] Denn diese Zwecke dürften regelmäßig nicht im Interesse des Auftraggebers liegen und somit dürfte mangels Zweckkomplementarität auch keine implizite Billigung anzunehmen sein. Soweit die Daten aus dem Kontext einer beruflichen Verarbeitung stammen, ist zudem die Haushaltsausnahme aus Art. 2 Abs. 2 lit. c DSGVO nicht anwendbar.[659] Denkbar sind als Folge des Auftragsverarbeiterexzesses also zwei Verantwortlichkeitsszenarien. Zum einen kann der ursprüngliche Auftragsverarbeiter als singulär Verantwortlicher für seine eigene Verarbeitung zu behandeln sein. Zum anderen kann, wenn der Entscheidungsbeitrag des ursprünglichen Auftragsverarbeiters durch den Auftraggeber sich zu eigen gemacht oder explizit oder implizit gebilligt wird, auch eine gemeinsame Verantwortlichkeit bestehen. Im Falle der Billigung wären dann gemeinsame Mittel erforderlich.[660] Diese dürften bei einer Auftragsverarbeitung aber regelmäßig vorliegen.

Ein Folgeproblem des Auftragsverarbeiterexzesses stellt die Verwendung der Daten des ursprünglichen Auftraggebers durch den Auftragsverarbeiter für weitere Auftragsverarbeitungen mit neuen Auftraggebern dar. Da die neuen Auftraggeber keine rechtmäßige Weisung für die Verwendung der Daten des ursprünglichen Auftraggebers geben können, kann insofern auch keine Privilegierung der Verarbeitung über eine Auftragsverarbeitung für den Auftragsverarbeiter bestehen. Zumindest für die weitere Speicherung und/oder Verschmelzung der Daten des ursprünglichen Auftraggebers mit seinen eigenen Daten ist der Auftragsverarbeiter also Verantwortlicher. Ein denkbarer Anwendungsfall hierfür wäre das Trainieren eines LLMs durch den Auftragsverarbeiter mit personenbezogenen Daten des Auftraggebers.

III. Funktionsübertragung und Auftragsverarbeiterexzess

Da die DSRL und das BDSG a.F. keine Art. 28 Abs. 10 DSGVO entsprechende Norm kannten, wurde die Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter unter anderem anhand des Kriteriums der Funktionsübertragung vorgenommen. Eine

[656] Nach *Cimina*, ERA Forum 2020, 5 muss die Entscheidung über den Vorschlag des Auftragsverarbeiters letztlich beim Verantwortlichen liegen.
[657] Zum Mitarbeiterexzess siehe unten.
[658] Mit einer Auflistung von Beispielsfällen: *Ambrock*, ZD 2020, 492, 494.
[659] Dazu: Kapitel 5 I. Haushaltsausnahme; *Ambrock*, ZD 2020, 492, 494 f.
[660] Ein gemeinsamer Zweck liegt ja gerade nicht vor.

Funktionsübertragung vom Auftraggeber auf den Auftragnehmer – der dann allerdings kein Auftragsverarbeiter, sondern Verantwortlicher war – lag demnach dann vor, wenn der Auftragnehmer eine relevante Eigenständigkeit im Hinblick auf die Verarbeitung aufwies.[661] Neben der technischen Durchführung der Verarbeitung mussten dabei umfassende vertragliche Leistungen durch die Verarbeitung erbracht werden oder ein Eigeninteresse des Auftragnehmers an der Verarbeitung vorliegen. Dieses Kriterium ist allerdings mit der expliziten Normierung des Auftragsverarbeiterexzesses in Art. 28 Abs. 10 DSGVO obsolet. In Fällen der Funktionsübertragung, die nicht im Einklang mit Art. 28 Abs. 10 DSGVO noch als Auftragsverarbeitung gewertet werden können, dürfte es sich nunmehr regelmäßig um gemeinsame Verantwortlichkeiten handeln.[662]

IV. Gesetzliche Übermittlungspflichten des Auftragsverarbeiters

Problematisch in Bezug auf den Auftragsverarbeiterexzess erscheinen Verarbeitungsszenarien, in denen ein Auftragsverarbeiter außerhalb der Auftragsverarbeitung zur Datenübermittlung an staatliche Stellen verpflichtet ist. Die Art. 29-Datenschutzgruppe illustrierte dies im WP 169 anhand des Beispiels von SWIFT,[663] einem internationalen Finanzdienstleister. Finanzinstitute schlossen mit SWIFT Auftragsverarbeitungsverträge ab, nach denen SWIFT für diese Institute Daten für kommerzielle Zwecke verarbeiten sollte. Nachdem SWIFT vom US-amerikanischen Finanzministerium per Verwaltungsakt dazu aufgefordert worden war, auch für die Zwecke der Bekämpfung der Finanzierung terroristischer Aktivitäten personenbezogene Daten aus den Auftragsverarbeitungen für die Finanzinstitute bereitzustellen, entschloss sich SWIFT, dieser Aufforderung nachzukommen. Damit setzte sich SWIFT aber über die Zweckbestimmung der Finanzinstitute hinweg und eröffnete mit dem US-amerikanischen Finanzministerium einem weiteren Akteur Zugang zu den Daten. Folglich lag, ungeachtet der vertraglichen Festlegung, ein Auftragsverarbeiterexzess vor und SWIFT übernahm damit für die Übermittlung der Daten an das US-amerikanische Finanzministerium die Rolle eines Verantwortlichen.

Zwar sieht die DSGVO mittlerweile für Übermittlungspflichten an staatliche Stellen eine Ausnahme von der Weisungsgebundenheit des Auftragsverarbeiters gem. Art. 28 Abs. 3 lit. a und Art. 29 DSGVO vor. Diese Ausnahme gilt allerdings nur für

---

[661] Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 15 ff.

[662] Sydow/Marsch/*Ingold*, Art. 28 DSGVO, Rn. 16, 26; Kühling/Buchner/*Hartung*, Art. 28 DSGVO, Rn. 43 ff.; Paal/Pauly/*Martini*, Art. 28 DSGVO, Rn. 7; *Dovas*, ZD 2016, 512, 517.

[663] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 14.

eine Übermittlungspflicht nach mitgliedstaatlichem oder Unionsrecht.[664] Für Verpflichtungen zur Übermittlung durch das Recht von Drittländern gilt die Privilegierung gerade nicht. Der Auftragsverarbeiter hat in diesem Fall nur die Wahl, entweder gegen das Recht des Drittlandes oder aber gegen die DSGVO zu verstoßen, sofern das Unionsrecht nicht die Übermittlung anderweitig rechtfertigt. Daneben stellt sich zudem die Frage, ob die Hinweispflicht des Auftragsverarbeiters gem. Art. 28 Abs. 3 lit. a DSGVO für eine Verarbeitungspflicht nach mitgliedstaatlichem oder Unionsrecht auch für eine solche Pflicht nach dem Recht eines Drittlands besteht. Im Rahmen eines Erst-Recht-Schlusses dürfte dies der Fall sein.

Die Entscheidung über die Zwecke und Mittel der Verarbeitung erschöpft sich in diesem Fall in der Erfüllung der Übermittlungspflicht gegenüber dem Drittland. Trotzdem erwächst hieraus eine Verantwortlichkeit für den Auftragsverarbeiter. Diese Situation ist für den Auftragsverarbeiter kaum haltbar und sollte de lege ferenda durch eine zentrale Stelle der EU oder der Mitgliedstaaten übernommen werden, die solche Übermittlungen entweder billigt oder verweigert. Die Stelle könnte etwa bei der Kommission angesiedelt werden. Eine gemeinsame Verantwortlichkeit des Auftragsverarbeiters mit der staatlichen Stelle des Drittlandes besteht, wie bei jeder anderen Übermittlungspflicht etwa nach Art. 6 Abs. 1 lit. c DSGVO, hingegen nicht.

V. Mitarbeiterexzess

Das Konzept des Mitarbeiterexzesses[665] ähnelt stark dem Auftragsverarbeiterexzess.[666] Daher können die Ausführungen zum Auftragsverarbeiterexzess grundsätzlich auch für den Mitarbeiterexzess übernommen werden. Ein Mitarbeiterexzess liegt dann vor,

[664] Art. 28 Abs. 3 lit. c DSGVO: „[...] die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen - auch in Bezug auf die Übermittlung personenbezogener Daten an ein **Drittland** oder eine **internationale Organisation** - verarbeitet, sofern er nicht durch das **Recht der Union oder der Mitgliedstaaten**, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;“ (Hervorhebung durch den Autor).

[665] Mit dem Begriff Mitarbeiter ist dabei die „unterstellte Person“ aus Art. 29 DSGVO gemeint. Ausführlich hierzu: *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 88 f.

[666] Taeger/Gabel/*Lutz/Gabel*, Art. 29 DSGVO, Rn. 18; Kühling/Buchner/*Hartung*, Art. 29 DSGVO, Rn. 16, 20. Paal/Pauly/*Martini*, Art. 29 DSGVO, Rn. 29c problematisiert hier eine Analogie zu Art. 28 Abs. 10 DSGVO. Sofern aber Art. 28 Abs. 10 DSGVO ggü. Art. 4 Nr. 7 DSGVO nur deklaratorisch wirkt, wäre der Mitarbeiter bereits nach dieser Definition ein eigener Verantwortlicher.

wenn eine dem Verantwortlichen unterstellte Person[667] entgegen seiner Weisung personenbezogene Daten verarbeitet.[668] Die Art. 29-Datenschutzgruppe scheint einen Mitarbeiterexzess vor allem dann anzunehmen, wenn eine natürliche Person personenbezogene Daten außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle des Arbeitgebers bzw. der juristischen Person für die sie handelt, für eigene Zwecke verarbeitet.[669] Illustrativ für den Mitarbeiterexzess ist Beispiel 4[670] (Heimliche Überwachung von Mitarbeitern) in WP 169. In diesem Beispiel veranlasst das Vorstandsmitglied eines Unternehmens die heimliche Überwachung der Mitarbeiter des Unternehmens ohne eine formelle Entscheidung des Vorstandes. Nach Ansicht der Art. 29-Datenschutzgruppe sei zunächst das Unternehmen als Verantwortlicher für die heimliche Überwachung der Mitarbeiter anzusehen. Das Vorstandsmitglied selbst solle dann Verantwortlicher sein, wenn es die erhobenen Daten zur Erzwingung persönlicher Gefälligkeiten von Mitarbeitern nutze. Die Verantwortlichkeit und Haftung des Unternehmens begründe sich aus den mangelnden Sicherheits- und Vertraulichkeitsmaßnahmen.[671] Der EDPB nimmt in einem solchen Fall eine Verletzung der Pflicht zur Ergreifung technischer und organisatorischer Maßnahmen nach Art. 24 Abs. 1 DSGVO an.[672] Soweit bekannt, liegt bislang nur eine deutschsprachige Entscheidung zum Mitarbeiterexzess vor.[673] Diese bezieht sich in ihrer Begründung auf die Leitlinien des EDPB. Der EuGH hat sich bislang nur dazu verhalten, ob sich ein Unternehmen im Rahmen eines Schadensersatzanspruches auf die Befreiung gem. Art. 82 Abs. 3 DSGVO berufen kann, wenn sich ihm unterstellte Personen gem. Art. 29 DSGVO weisungswidrig verhalten hat.[674] Dies hat der EuGH verneint. Die Entscheidung ist damit im Einklang mit der

[667] Vgl. zum Anwendungsbereich S/J/T/K/*Kremer*, Art. 29 DSGVO, Rn. 7 f.; BeckOK DatenschutzR[47]/*Spoerr*, Art. 29 DSGVO, Rn. 11. Kühling/Buchner/*Hartung*, Art. 29 DS-GVO, Rn. 14 zur Frage, ob damit a. juristische Personen erfasst werden.

[668] Sydow/Marsch/*Ziebarth*, Art. 4 Nr. 10 DSGVO, Rn. 162; Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 177, 282. Vgl. Art. 29 DSGVO, dazu: Kuner/Bygrave/Docksey/*Millard/Kamarinou*, Art. 29 GDPR, 614 f.; Kühling/Buchner/*Hartung*, Art. 29 DS-GVO, Rn. 2. Ähnlich wohl: BeckOK DatenschutzR[47]/*Schild*, Art. 4 DSGVO, Rn. 121.

[669] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 88.

[670] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 21.

[671] Ebenso: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 19.

[672] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 19 Fn. 12. Sydow/Marsch/*Mantz*, Art. 32 DSGVO, Rn. 25 f.

[673] ÖBVwG, Erkenntnis vom 21.12.2021 – W258 2238615-1/16E = ZD 2022, 439.

[674] EuGH, Urteil vom 11.04.2024 – C-741/21 (Juris), Rn. 44 ff.

Regelung zum Auftragsverarbeiterexzess in Art. 28 Abs. 10 DSGVO, der einen Schadensersatzanspruch auch gegen den Auftraggeber als ursprünglich Verantwortlichen vorsieht, unbeschadet einer eigenen Verantwortlichkeit des ursprünglichen Auftragsverarbeiters (im Exzess).

Nach Ansicht der deutschen Aufsichtsbehörden soll die Analyse der Zurechenbarkeit des Verhaltens eines Mitarbeiters objektiv erfolgen, also nicht subjektiv aus Sicht des Verantwortlichen.[675] Entscheidend sei die objektive Zweckbestimmung der dem Mitarbeiter zugewiesenen Aufgaben. Überschreite ein Mitarbeiter seine internen Befugnisse, sei dies solange unschädlich, wie dies objektiv zur Förderung der wirtschaftlichen Interessen des Unternehmens geschehe. Worauf die objektive Analyse des Exzesses anhand des Zweckes der Verarbeitung beruht oder welche Vorteile sie haben soll, wird allerdings nicht klar. Sofern sich ein Mitarbeiter im Rahmen des Entscheidungsspielraums, den ihm der Verantwortliche zugesteht, bewegt, handelt er im Rahmen der Entscheidung über die Zwecke und Mittel des Verantwortlichen. Bewegt er sich hingegen außerhalb dieses Spielraums und entscheidet er eigenmächtig über die Zwecke und Mittel der Verarbeitung, gleichwohl aber im Interesse des Verantwortlichen, liegt grundsätzlich eine eigene Entscheidung über Zwecke und Mittel der Verarbeitung vor. Dies muss im Hinblick auf Art. 29 DSGVO unabhängig von der Zweckvereinbarkeit der Entscheidung des Mitarbeiters gelten.[676] Maßgeblich sind zur Bestimmung des Exzesses also weniger die Aufgaben als der Entscheidungsspielraum des Mitarbeiters.[677] Denkbar könnte höchstens sein, dass sich der Verantwortliche eine Entscheidung des Mitarbeiters zu eigen macht oder diese explizit oder implizit billigt. Der Ansatz einer objektiven Analyse der Aufsichtsbehörden mit Fokus auf den Zweck der Verarbeitung und die Aufgaben des Mitarbeiters erscheint daher vor allem als eine pragmatische Herangehensweise.

Teilweise wird vertreten, dass eine indirekte Exkulpationspflicht der Stelle (also des vermeintlich Verantwortlichen oder Auftragsverarbeiters), der der Mitarbeiter grundsätzlich zuzurechnen ist, bestehen soll, sofern ein Mitarbeiter seine eigenen Befugnisse

[675] *Ambrock*, ZD 2020, 492, 493. Ähnlich *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 17 für den Auftragsverarbeiterexzess. Demnach soll ein Exzess nach Art. 28 Abs. 10 DSGVO u.a. davon abhängen, wodurch die Abweichung motiviert war, etwa eine Abweichung im Bereich der Mittel mit dem Ziel der Einhaltung der Datenschutzgrundsätze.

[676] Vgl. zum Auftragsverarbeiterexzess *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 56.

[677] Anders: *Ambrock*, ZD 2020, 492, 493. Dementsprechend scheint a. die Schlussfolgerung, dass Lehrer im Rahmen ihrer Unterrichtstätigkeit hinsichtlich der Mittel der Verarbeitung freie Wahl haben, unzutreffend: ebd., 494.

überschreitet.[678] Das ist aber nicht nachzuvollziehen, denn die Untersuchung der Umstände, die die Verantwortlichkeit begründen, ist Aufgabe der Aufsichtsbehörde. Diese Aufgabe folgt daraus, dass die Verantwortlichkeit regelmäßig Voraussetzung der Abhilfebefugnisse ist. Um die Verantwortlichkeit festzustellen, kann die Aufsichtsbehörde auf ihre Untersuchungsbefugnisse zurückgreifen. Eine indirekte Exkulpationspflicht der maßgeblichen Stelle bezüglich des Verhaltens eines Mitarbeiters ist normativ nicht zu begründen. Es stellt vielmehr eine Obliegenheit der Stelle dar, entsprechende Informationen an die Aufsichtsbehörde zu geben, die eine eigene Verantwortlichkeit des Mitarbeiters darlegen.

VI. Fazit

Sowohl ein Auftragsverarbeiterexzess als auch ein Mitarbeiterexzess kann, muss aber nicht zu einer gemeinsamen Verantwortlichkeit führen. Damit eine gemeinsame Verantwortlichkeit eines ursprünglichen Auftragsverarbeiters und des Auftraggebers festgestellt werden kann, muss zunächst ein Wille zur Zusammenarbeit im Rahmen der Billigung der fremden Entscheidungsbeiträge zu dem nicht gemeinsamen Element, regelmäßig wohl der jeweiligen Zwecke, festgestellt werden. Alternativ wäre auch ein Zu-Eigen-Machen des fremden Entscheidungsbeitrags denkbar. Entsprechendes gilt für den Mitarbeiter im Exzess.

L. Folgen der gemeinsamen Verantwortlichkeit

Schwerpunkt dieser Arbeit sind, wie bereits erwähnt, die Voraussetzungen der Verantwortlichkeit.[679] Gerade bei der gemeinsamen Verantwortlichkeit besteht aber eine systematische Wechselwirkung zwischen ihren Folgen und Voraussetzungen. Denn sofern eine gemeinsame Verantwortlichkeit auch Vorteile für die gemeinsam Verantwortlichen bringt, liegt es nahe, ihre Voraussetzungen flexibler zu verstehen. Daher sind auch die Folgen der gemeinsamen Verantwortlichkeit zu beleuchten. Zu diesen Folgen gehört primär die Frage, ob gemeinsam Verantwortliche gegenüber singulär Verantwortlichen hinsichtlich einer internen Übermittlung privilegiert sind. Ebenso stellt sich die Frage, wie die Reichweite und der Anteil der Verantwortlichkeit eines individuellen gemeinsam Verantwortlichen zu begrenzen sind, insbesondere falls keine Privilegierung

[678] So: *Ambrock*, ZD 2020, 492, 493.
[679] Dazu:
Kapitel 3.

der gemeinsam Verantwortlichen besteht. Dabei bezieht sich die Reichweite der Verantwortlichkeit auf die Verarbeitungsvorgänge, die von einer Verantwortlichkeit erfasst sind. Der Anteil der Verantwortlichkeit wiederum bezieht sich auf den Grad einer Beteiligung an einem konkreten Verarbeitungsvorgang. Weiter stellt sich die Frage, ob gemeinsam Verantwortliche Pflichten aus der DSGVO autonom erfüllen können müssen oder ob eine Delegation von Pflichten unter gemeinsam Verantwortlichen möglich ist. In diesem Zusammenhang ist auch fraglich, ob Art. 26 Abs. 3 DSGVO eine „Gesamtschuld" hinsichtlich der Pflichten anordnet. Schließlich stellt sich die Frage, wie seitens der Aufsichtsbehörden eine Störerauswahl unter gemeinsam Verantwortlichen zu erfolgen hat.

I. Privilegierung der Übermittlung zwischen gemeinsam Verantwortlichen?

Teilweise wird bei der gemeinsamen Verantwortlichkeit, ähnlich zur Auftragsverarbeitung,[680] angenommen, dass eine Übermittlung zwischen gemeinsam Verantwortlichen insofern privilegiert sein solle, dass keine zusätzliche Verarbeitungsrechtfertigung nach Art. 6 Abs. 1 DSGVO notwendig sei.[681] Ausgangspunkt für diese Annahme soll die Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO selbst sein. Sie lautet (verkürzt) wie folgt: „die [...] Stelle, die [...] gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet; [...]". Dabei lässt sich der Definitionsteil „anderen" über die Definition des Dritten in Art. 4 Nr. 10 DSGVO ableiten: „eine [...] Stelle, außer [...] dem Verantwortlichen [...]". Geht man davon aus, dass die Definition des Verantwortlichen im Rahmen des „gemeinsam mit anderen" neben dem individuellen gemeinsam Verantwortlichen auch die weiteren gemeinsam Verantwortlichen einschließt, wären die anderen gemeinsam Verantwortlichen nach der Definition des Dritten eben keine Dritten.[682] Der Teil der Definition des Dritten

[680] Hierzu: *Kremer*, CR 2019, 225, Rn. 33 ff.

[681] Vgl. den Überblick bei *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 167 ff. Noch in der 2.Aufl.: Gola/*Piltz*, Art. 26 DSGVO, Rn. 8; Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 3a; *Kremer*, CR 2019, 225, Rn. 36 ff.; ablehnend: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 167 Fn. 76; Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 62; Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 23; *Monreal*, CR 2019, 797, Rn. 50; S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 63 ff. Unklar: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 46.

[682] Die Art. 29-Datenschutzgruppe verhielt sich in WP 169 im Rahmen des Dritten leider nicht zur gemeinsamen Verantwortlichkeit: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 37. Gleiches gilt für den EDPB: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 85 ff.

„[...] außer [...] dem Verantwortlichen [...]“ würde also mit dem Verantwortlichen alle gemeinsam Verantwortlichen beinhalten. Folglich wäre eine Übermittlung an die anderen gemeinsam Verantwortlichen auch keine Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO, die einer Verarbeitungsrechtfertigung nach Art. 6 Abs. 1 DSGVO bedürfte.[683] Es würde sich vielmehr um eine „Übermittlung“ innerhalb der eigenen Organisationseinheit[684] handeln.[685] Wären also etwa Teile eines Konzerns, i.S.v. Tochtergesellschaften, mit der Muttergesellschaft zusammen gemeinsam Verantwortliche, wäre unter Annahme einer solchen Privilegierung keine Verarbeitungsrechtfertigung notwendig.

1. Wortlaut der Definition

Ob die Definition der gemeinsam Verantwortlichen aber Anlass für eine solche Privilegierung gibt, ist fraglich.[686] So definiert Art. 4 Nr. 7 DSGVO gleichzeitig den singulär Verantwortlichen wie auch den gemeinsam Verantwortlichen. Rein grammatikalisch müssen sich also Teile der Definition sowohl auf den singulär Verantwortlichen wie auch den gemeinsam Verantwortlichen beziehen können. Ob sich daraus etwas für die Frage, ob eine gemeinsame Verantwortlichkeit im Sinne einer einzelnen Rechtsfigur[687] oder aber zwei (oder mehr) individuelle Verantwortliche, die in gewisser Weise verbunden sind, vorliegen, ableiten lässt, bleibt unklar. Grundsätzlich wäre es allerdings sinnvoll gewesen, die Definition um „[...] gemeinsam mit anderen **Verantwortlichen** [...] entscheidet; [...]“ zu ergänzen, wenn ein Verständnis intendiert ist, in dem die gemeinsam Verantwortlichen nicht zu einer einzigen „Verantwortlichkeitsmasse“ zusammenschmelzen. Ohne eine solche Ergänzung bleibt unklar, ob das „gemeinsam mit anderen“ alle gemeinsam Verantwortlichen in einer Organisationseinheit einschließt oder nicht.[688] Auch die Definition der gemeinsam Verantwortlichen in Art. 26 Abs. 1 S. 1 DSGVO schafft keine weitere Klarheit. Nach dieser Definition sind zwei (oder mehr)

[683] Vgl. in der 2. Aufl.: Gola/*Piltz*, Art. 26 DSGVO, Rn. 8.

[684] I.S.v. Stelle.

[685] Unklar: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24. Aufgrund der dortigen Formulierung („ [...] nur als Datenübermittlung [...]“) stellt sich im Umkehrschluss die Frage, ob ein Austausch zwischen zwei gemeinsam Verantwortlichen dann keine Datenübermittlung und somit hinsichtlich einer Verarbeitungsrechtfertigung privilegiert wäre.

[686] A. *Monreal*, CR 2019, 797, Rn. 50 hat diese Position in Anbetracht der jüngeren Rechtsprechung des EuGH mittlerweile aufgegeben.

[687] Dazu: Kapitel 4 C. IV. Gemeinsam Verantwortliche als Rechtssubjekt sui generis?

[688] Ebenso lassen sich a. aus ErwGr 79 DSGVO keine klaren Schlüsse für oder gegen eine Privilegierung ziehen. A.A. wohl aber: *Schreiber*, ZD 2019, 55, 55.

Verantwortliche dann gemeinsam Verantwortliche, wenn sie die Zwecke der und die Mittel zur Verarbeitung gemeinsam festlegen. Ob die gemeinsam Verantwortlichen im Verhältnis zueinander Dritte sind, wird durch die Qualifizierung der Verantwortlichen als gemeinsam Verantwortliche nicht klar. Deutlich wird nur eine gewisse Verbundenheit.

2. Umkehrschluss aus Folgen der Verantwortlichkeit

Neben der Definition der gemeinsam Verantwortlichen lässt sich auch aus den Folgen einer gemeinsamen Verantwortlichkeit eine Privilegierung kaum herleiten. Die Betroffenenrechte können gem. Art. 26 Abs. 3 DSGVO gegenüber jedem individuellen gemeinsam Verantwortlichen geltend gemacht werden. Ebenso verlangt der EuGH, dass jeder gemeinsam Verantwortliche eine Verarbeitungsrechtfertigung nachweisen muss.[689] Art. 82 Abs. 4 DSGVO wiederum ordnet eine Gesamtschuld bei mehreren beteiligten Verantwortlichen an einer Verarbeitung an. Diese undifferenzierte Inanspruchnahme aller gemeinsam Verantwortlichen könnte zwei Rückschlüsse zulassen. Zum einen, dass entweder nicht individuelle gemeinsam Verantwortliche vorliegen, sondern eine einheitliche Rechtsfigur der gemeinsamen Verantwortlichkeit. Zum anderen könnte man hieraus den Schluss ziehen, dass die gemeinsam Verantwortlichen untereinander jedenfalls eine Privilegierung genießen. Denn grundsätzlich wäre es denkbar, dass etwa durch das zusätzliche Risiko einer Gesamtschuld auch Vorteile für gemeinsam Verantwortliche entstehen, ähnlich wie der Auftragsverarbeiter durch seine Weisungsgebundenheit hinsichtlich einer Verarbeitungsrechtfertigung privilegiert ist.[690] Andererseits bürdet Art. 82 Abs. 4 DSGVO den Schadensersatz aber nicht der „gemeinsamen Verantwortlichkeit" als solcher auf, sondern bildet nur eine Gesamtschuld der beteiligten Verantwortlichen. Diese „beteiligten Verantwortlichen" müssen streng nach dem Wortlaut nicht einmal gemeinsam Verantwortliche sein, denn Auslöser für die Gesamtschuld ist bereits die Beteiligung an derselben Verarbeitung.[691] Es gilt also immer noch der Grundsatz, dass jeder (einzelne) an einer Verarbeitung beteiligte Verantwortliche nach Art. 82 Abs. 2 S. 1 DSGVO haftet. Auch bei Art. 26 Abs. 3 DSGVO wird die interne Vereinbarung der gemeinsam Verantwortlichen nur nach außen hin modifiziert. So kann die betroffene Person zwar bei jedem einzelnen der ge-

[689] S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 67.
[690] Dazu unten.
[691] Sydow/Marsch/*Kreße*, Art. 82 DSGVO, Rn. 22.

meinsam Verantwortlichen ihre Rechte geltend machen. Allerdings sagt diese Geltendmachung nichts darüber aus, wer diese Rechte letztlich erfüllt.[692] Insgesamt fällt bei Art. 26 Abs. 3 und 82 Abs. 4 DSGVO somit zweierlei auf: Zum einen sprechen beide Artikel von individuellen Verantwortlichen und nicht von einer gemeinsamen Einheit.[693] Gemeinsam Verantwortliche sind also nur eine Mehrzahl von Verantwortlichen, die sich durch eine gewisse Nähebeziehung auszeichnen. Zum anderen privilegieren beide Normen nur die betroffene Person.[694] Diese Modifikation des jeweiligen Grundsatzes zugunsten der betroffenen Person dürfte dadurch begründet sein, dass zum einen die betroffene Person nicht einem Zuständigkeits-„Ping-Pong"[695] zum Opfer fallen soll, zum anderen, dass der betroffenen Person nicht das Prozessrisiko bei einem Schadensersatz aufgebürdet werden soll.[696]

3. Vergleich zum Auftragsverarbeiter

Vergleicht man die gemeinsame Verantwortlichkeit mit der Auftragsverarbeitung, fällt auf, dass beide Konzepte zwar eine Vereinbarung bzw. einen Vertrag verlangen. Im Gegensatz zur Vereinbarung nach Art. 26 Abs. 1 DSGVO enthält der Vertrag nach Art. 28 Abs. 3 DSGVO aber sehr viel detailliertere Vorgaben hinsichtlich des Inhalts. Daneben stellt Art. 29 DSGVO ausdrücklich klar, dass die Verarbeitung von personenbezogenen Daten nur auf Weisung des Verantwortlichen stattfinden kann. Eine vergleichbare Kontrolle hat ein individueller gemeinsam Verantwortlicher, außerhalb potenzieller Abreden im Innenverhältnis, nicht gegenüber den anderen gemeinsam Verantwortlichen.[697] Folglich gibt es auch keine Entsprechung des Auftragsverarbeiterexzesses in Art. 28 Abs. 10 DSGVO für die gemeinsam Verantwortlichen. Die Sanktion einer Überschreitung der Befugnisse eines individuellen gemeinsam Verantwortlichen kann nur im Innenverhältnis der gemeinsam Verantwortlichen, etwa aus einem Vertrag heraus, erfolgen. Für die Geltendmachung der Betroffenenrechte in Art. 26 Abs. 3

[692] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 165: „[...] may contact either of the joint controllers [...]".

[693] Art. 26 DSGVO schafft also kein neues Zuordnungssubjekt sui generis, siehe a.: Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 24.

[694] *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 507. So gilt eine gesamtschuldnerische Haftung a. nicht für Geldbußen nach Art. 83 Abs. 4 lit. a DSGVO.

[695] Simitis/Hornung/Spiecker/*Petri*, Art. 26 DSGVO, Rn. 28; *Mester/Öztürk*, DuD 2023, 73, 74.

[696] Art. 26 Abs. 3 DSGVO erkennt also scheinbar an, dass die betroffene Person trotz der Vereinbarung aus Abs. 2 mit der Analyse des Sachverhalts überfordert sein könnte und relativiert diese interne Zuständigkeitsregelung nach außen. Siehe a.: *Hacker*, MMR 2018, 779, 780.

[697] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 173.

DSGVO findet sich ebenfalls keine Entsprechung für den Auftragsverarbeiter. Aufgrund der Weisungsgebundenheit ist der Auftragsverarbeiter im Gegensatz zum gemeinsam Verantwortlichen nach Art. 82 Abs. 2 S. 2 DSGVO in der Haftung privilegiert. Daneben gilt die Gesamtschuld in Art. 82 Abs. 4 DSGVO im Übrigen aber auch für den Auftragsverarbeiter, sofern er gem. Art. 82 Abs. 2 S. 2 DSGVO überhaupt haftet.

Geht man davon aus, dass das datenschutzrechtliche Attributionsmodell der Verantwortlichkeit organisations- und hierarchie-orientiert ist, ergibt es insgesamt keinen Sinn den gemeinsam Verantwortlichen ebenso wie den Auftragsverarbeiter zu privilegieren. Prototyp der Verantwortlichkeit ist nach wie vor der singulär Verantwortliche, der entweder innerhalb seiner Organisationseinheit[698] oder durch das Auftragsverarbeitungsverhältnis Weisungen erteilen kann.

4. Abgrenzung der Übermittlung von einer gemeinsamen Erhebung

Von der Privilegierung einer Übermittlung zwischen gemeinsam Verantwortlichen ist schließlich das Szenario zu unterscheiden, in dem mehrere gemeinsam Verantwortliche bereits gemeinsam Daten erheben. Denn dann wäre die jeweilige Erhebung dieser Verantwortlichen bereits gem. Art. 6 Abs. 1 DSGVO zu rechtfertigen.[699] Da aber nach der Rechtsprechung des EuGH nicht jeder gemeinsam Verantwortliche Zugriff auf die personenbezogenen Daten haben muss,[700] also auch nicht notwendigerweise eine gemeinsame Erhebung oder Speicherung vorliegen muss, wird für eine spätere Übermittlung zwischen den gemeinsam Verantwortlichen wieder eine Verarbeitungsrechtfertigung notwendig.[701]

5. Bewertung

Trotz dieser gewichtigen Argumente scheint es aus Sicht eines Verantwortlichen unbefriedigend, dass im Rahmen einer gemeinsamen Verantwortlichkeit, abseits der internen Verteilung bestimmter Pflichten nach Art. 26 Abs. 1 S. 2 DSGVO,[702] keine Vorteile

---

[698] I.S.d. Stelle.

[699] So scheinbar a.: BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 43; *Monreal*, CR 2019, 797, Rn. 50 im Hinblick auf gemeinsam genutzte Infrastruktur.

[700] Zuletzt bestätigt in: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 69.

[701] Vgl. BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 45.

[702] Dazu: Kapitel 4 L. V. Delegation von Pflichten zwischen gemeinsam Verantwortlichen.

bestehen.[703] So kann weder auf eine einheitliche Verarbeitungsrechtfertigung nach Art. 6 Abs. 1 DSGVO zurückgegriffen werden,[704] noch bildet Art. 26 DSGVO selbst eine Verarbeitungsrechtfertigung.[705] Betrachtet man die Regelung der gemeinsamen Verantwortlichkeit unter dem damit verbundenen Bußgeldrisiko in Art. 83 Abs. 4 lit. a DSGVO, soll möglicherweise aber auch nur die Verarbeitungsrealität[706] transparent abgebildet werden und nicht ein Anreiz zur gemeinsamen Verantwortlichkeit geschaffen werden. Denn insgesamt dienen die Pflichten, die sich aus Art. 26 DSGVO ergeben, nicht den gemeinsam Verantwortlichen, sondern der betroffenen Person.[707]

II. Reichweite und Anteil der individuellen Verantwortlichkeit

Soweit keine Privilegierung der gemeinsamen Verantwortlichkeit besteht, ist umgekehrt maßgeblich, wie weit die individuelle Verantwortlichkeit eines gemeinsam Verantwortlichen reicht und wie sich innerhalb dieser Verantwortlichkeit sein Anteil an der Verantwortung bemisst. Die Reichweite der Verantwortlichkeit bestimmt nämlich, für welche Verarbeitungen der individuelle gemeinsam Verantwortliche verantwortlich im Sinne der Pflichten der DSGVO ist und für welche Verarbeitungen er haftet. Damit stellt sich auch die Frage, inwiefern ein individueller gemeinsam Verantwortlicher auch für vor- oder nachgelagerte Verarbeitungen der anderen gemeinsam Verantwortlichen verantwortlich ist. Der Anteil der Verantwortlichkeit ist wiederum für die Berechnung von Schadensersatz und die Höhe einer Geldbuße relevant.

1. Ansatzpunkt für die Reichweite der Verantwortlichkeit

Dabei stellt sich zunächst die Frage, was überhaupt Abgrenzungskriterium für die Reichweite der Verantwortlichkeit ist. Anhand der Definition des Verantwortlichen in

[703] So schlagen *Lee/Cross*, MMR 2019, 559, 562 a. getrennt Verantwortliche statt gemeinsam Verantwortlicher vor.

[704] Die Verarbeitungsrechtfertigung muss vielmehr jeweils für den individuellen gemeinsam Verantwortlichen festgestellt werden. Dabei ist eine Identität der Verarbeitungsrechtfertigung nicht ausgeschlossen, andererseits aber a. nicht grundsätzlich anzunehmen. Siehe a.: Simitis/Hornung/Spiecker/*Petri*, Art. 26 DSGVO, Rn. 1.

[705] *Monreal*, CR 2019, 797, Rn. 50; *Dovas*, ZD 2016, 512, 515.

[706] Vgl. Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 2. Siehe a.: *Monreal*, CR 2019, 797, Rn. 54: „[...] weder eine Privilegierung noch eine Diskriminierung [...]". Allgemein zur Intransparenz: *Roßnagel*, MMR 2005, 71, 72.

[707] Siehe *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 506, die „den vollumfängliche[n] Betroffenenschutz" als Sinn und Zweck der Norm ansehen. Ähnlich: *Dovas*, ZD 2016, 512, 514; *Reif*, RdV 2019, 30, 31 m.w.N. Vgl. a. *Spiecker gen. Döhmann*, CR 2016, 698, 703 f. zur Haftung im Rahmen systemischer Digitalisierung. Kritisch: Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 153.

Art. 4 Nr. 7 DSGVO ist Objekt der Entscheidung über Zwecke und Mittel die Verarbeitung.[708] Die Verarbeitung wiederum besteht nach der Definition in Art. 4 Nr. 2 DSGVO aus dem einzelnen Verarbeitungsvorgang oder der Vorgangsreihe. Eine Differenzierung der verschiedenen Vorgänge oder Vorgangsreihen ist nur in quantitativer Hinsicht notwendig, also ob es sich um unterschiedliche Vorgänge oder Vorgangsreihen handelt. Ob diese Vorgänge als Erhebung, Speicherung oder Übermittlung zu klassifizieren sind,[709] ist hingegen nicht von Bedeutung. Somit bezieht sich die Verantwortlichkeit grundsätzlich immer kleinteilig auf die konkreten, individuellen Vorgänge.[710] Diese individuellen Vorgänge können potenziell auch als Vorgangsreihe unter einem einheitlichen Zweck zusammengefasst werden. Maßgeblich für die Reichweite der individuellen Verantwortlichkeit eines gemeinsam Verantwortlichen ist definitionsgemäß also, über welche Vorgänge und Vorgangsreihen er gemeinsam (mit anderen) entscheidet.[711]

Dass sich die individuelle Verantwortlichkeit eines gemeinsam Verantwortlichen nur auf den konkreten Verarbeitungsvorgang bezieht, über den dieser Verantwortliche gemeinsam mitentscheidet, hat der EuGH im Urteil in der Rechtssache Fashion ID[712] deutlich gemacht: „Daraus folgt, [...] dass eine natürliche oder juristische Person offenbar nur für Vorgänge der Verarbeitung personenbezogener Daten, über deren Zwecke und Mittel sie – gemeinsam mit anderen – entscheidet, [...] gemeinsam mit anderen verantwortlich sein kann. Dagegen kann [...] diese natürliche oder juristische Person für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder die Zwecke noch die Mittel festlegt, nicht als [...] verantwortlich angesehen werden."[713] Die Verarbeitungsvorgänge, zu denen ein Entscheidungsbeitrag eines individuellen gemeinsam Verantwortlichen vorliegt, bilden demnach den Rahmen für dessen individuelle

[708] Dazu: Kapitel 2 A. Bezug zur Verarbeitung.

[709] Unglücklich formuliert: *Golland*, K&R 2019, 533, 534.

[710] Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO, Rn. 185. Beispielhaft: *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 46, 63, 82.

[711] *Mester/Öztürk*, DuD 2023, 73, 75. Sydow/Marsch/*Raschauer*, Art. 4 Nr. 7 DSGVO, Rn. 124, 126 möchte für die Verantwortlichkeit aber anscheinend a. die Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO berücksichtigen.

[712] Dazu: Kapitel 4 B. III. Fashion ID.

[713] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74.

Verantwortlichkeit.[714] Diese Bestimmung der Reichweite der individuellen Verantwortlichkeit wird in der Literatur als vorgangsorientierter Ansatz bezeichnet.[715] Bereits in der Rechtssache Google Spain hatte der EuGH, wenn auch etwas nebulöser, festgehalten, dass „der Suchmaschinenbetreiber daher in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür zu sorgen [hat], dass die Tätigkeit den Anforderungen der RL 95/46/EG entspricht."[716]

Eine ganz ähnliche Eingrenzung der individuellen Verantwortlichkeit des gemeinsam Verantwortlichen fand sich auch im WP 169 der Art. 29-Datenschutzgruppe. Objekt der „gemeinsamen Kontrolle" sei letztendlich die Verarbeitung als solche.[717] Dabei schließe die Definition des Verantwortlichen nicht aus, dass verschiedene Akteure an verschiedenen Vorgängen oder Vorgangsreihen und sowohl gleichzeitig als auch in verschiedenen Stadien beteiligt sein können.[718]

a) Der „Grad der Verantwortlichkeit" in der Rechtsprechung des EuGH

In den Entscheidungen des EuGH taucht seit dem Urteil in der Rechtssache Wirtschaftsakademie[719] der Begriff des „Grades der Verantwortlichkeit" regelmäßig auf, so zuletzt in der Rechtssache Fashion ID: „Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein, so dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist."[720] Dabei bleibt die Bedeutung des Begriffes des Grades generell unklar.[721] *Kosmider* etwa möchte den Grad der Verantwortlichkeit mit Verweis Art. 82 Abs. 2 lit. d DSGVO auf das Innenverhältnis der gemeinsam Verantwortlichen beziehen.[722] Da die

[714] *Monreal*, CR 2019, 797, Rn. 46; wohl a.: *Hanloser*, ZD 2019, 455, 459. Die Anknüpfung an einzelne Vorgänge, in Abgrenzung zu einer übergreifenden Verantwortlichkeit für Erhebung, Verarbeitung und Nutzung, ist im Übrigen nichts neues, sondern wurde bereits 1997 so vertreten: Dammann/Simitis DSRL/*Dammann*, Art. 2, Rn. 13; vgl. a. *Jung/Hansch*, ZD 2019, 143, 144.

[715] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 42 unterstreichen die Bedeutung dieses Ansatzes.

[716] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 38, 83.

[717] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[718] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 22.

[719] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[720] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70.

[721] So: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 57; *Schreiber*, ZD 2019, 55, 57; *Kollmar*, NVwZ 2019, 1740, 1740. Kritisch a.: *Moos/Rothkegel*, MMR 2019, 584, 586.

[722] *Kosmider*, Die Verantwortlichkeit im Datenschutz, 2021, 42 f.

maßgebliche Randnummer unmittelbar vor die Ausführungen des EuGH zum vorgangsorientierten Ansatz fällt, dürfte sie sich auch auf diesen beziehen.[723] Illustrativ hierzu sind auch die Schlussanträge des Generalanwalts in der Rechtssache Fashion ID ab Rn. 94: „Die Logik legt es daher nahe, die Frage der Verantwortlichkeit mit Blick auf den betreffenden konkreten Vorgang zu prüfen, und eben nicht mit Blick auf ein unbestimmtes Bündel von allem Möglichen, was als Verarbeitung bezeichnet werden kann."[724]

b) Kritik des vorgangsorientierten Ansatzes

Der Fokus des EuGH auf den individuellen Verarbeitungsvorgang[725] als Maßstab für die Reichweite der Verantwortlichkeit erweist sich allerdings als zweischneidiges Schwert. Zwar wird damit die Verantwortlichkeit der gemeinsam Verantwortlichen untereinander klar begrenzt, allerdings muss bei jeder Analyse der Verantwortlichkeit genau nach Vorgängen, wie auch Vorgangsreihen,[726] getrennt werden. Folge dieser Rechtsprechung dürften eine Vielzahl von „Micro-Joint-Controllerships" sein, samt entsprechender Vereinbarungen nach Art. 26 Abs. 1 S. 2 DSGVO.[727]

Problematisch am vorgangsorientierten Ansatz erscheint allerdings vor allem die Reduktion der Konsequenzen der Verarbeitung auf die einzelnen Vorgänge. Damit verliert der vorgangsorientierte Ansatz den Blick auf das „große Ganze" der Verarbeitung, also die Aggregation verschiedener Vorgänge und Datensätze.[728] Diese Aggregation und die daraus folgende Informationsasymmetrie wird mitunter als Ziel des Datenschutzes bezeichnet. Konsequenz des vorgangsorientierten Ansatzes ist bei komplexen Verarbeitungsszenarien jedenfalls ein erhebliches Defizit an Transparenz gegenüber der betroffenen Person. Diese Transparenz der Verarbeitung gegenüber der betroffenen Person wiederum stellt gem. Art. 5 Abs. 1 lit. a DSGVO einen der Grundsätze der Datenverarbeitung dar.[729] Der Transparenzgrundsatz gilt dabei insbesondere für die

[723] So a.: *Golland*, K&R 2019, 533, 534. Insofern geht die Annahme von intern vereinbarten „Abstufungen der Verantwortung" wohl fehl: *Hacker*, MMR 2018, 779, 780.

[724] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 99.

[725] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70-74, 76.

[726] Dies scheint in EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 72 unter den Tisch zu fallen. Daneben ist bislang a. höchstrichterlich nicht geklärt, was genau eine Vorgangsreihe ist.

[727] *Golland*, K&R 2019, 533, 536.

[728] Vgl. *Mahieu/van Hoboken*, https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/ (abgerufen am 17.07.2024). Kritisch a.: Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 38 f.; *Monreal*, CR 2019, 797, Rn. 47. Siehe zu dieser „Granularität" a.: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 13 f.

[729] Siehe a. ErwGr 39 DSGVO.

Informationen über den Zweck der Verarbeitung gem. Art. 13 Abs. 1 lit. c DSGVO. Auffangen lassen dürfte sich dieses Defizit an Transparenz allenfalls durch eine zusätzliche Pflicht zur Information über die Zwecke der Verarbeitung seitens der Empfänger der Daten gem. Art. 13 Abs. 1 lit. e DSGVO. Zwar wird auch das Informationsdefizit der gemeinsam Verantwortlichen untereinander durch die Beschränkung auf die gemeinsam determinierten Vorgänge berücksichtigt.[730] Allerdings könnte dieses Informationsdefizit auch durch einen Informationsanspruch der gemeinsam Verantwortlichen untereinander kompensiert werden. Nach aktueller Rechtslage geht das Informationsdefizit der gemeinsam Verantwortlichen untereinander aber zu Lasten der betroffenen Person.

Probleme ergeben sich aufgrund des vorgangsorientierten Ansatzes auch auf der praktischen Ebene. Denn Konsequenz dieses Fokus auf die konkreten Vorgänge ist, dass die Informationspflichten eines gemeinsam Verantwortlichen sich nur auf die von ihm verantworteten Vorgänge beziehen. Hat nun ein anderer gemeinsam Verantwortlicher keine Möglichkeit, eine betroffene Person unabhängig von diesem gemeinsam Verantwortlichen vor einer Verarbeitung zu informieren, stellt sich die Frage wie mit dieser fehlenden Informationsmöglichkeit umzugehen ist. Sofern keine nachgelagerten Verarbeitungsvorgänge seitens des anderen gemeinsam Verantwortlichen vorliegen, ist dieses Szenario unproblematisch. Denn dann müssen ohnehin alle gemeinsam Verantwortlichen über dieselben Verarbeitungsvorgänge informieren. Eine solche Identität der Verarbeitungsvorgänge zwischen den gemeinsam Verantwortlichen ist aber keinesfalls der Regelfall. Häufig wird es einen nur eingeschränkt gemeinsam Verantwortlichen geben, der direkten Kontakt mit der betroffenen Person hat, sowie einen weitergehend gemeinsam Verantwortlichen, der keine direkte Interaktionsmöglichkeit zur betroffenen Person besitzt. Ein solches Szenario zeigt sich etwa im Sachverhalt zu der Rechtssache Fashion ID.[731] Dort hatte der Plattformbetreiber, der das Social Plugin bereitstellte, das auf der Seite des Websitebetreibers eingebunden wurde, keine Möglichkeit die Besucher der Website des Websitebetreibers vor der Erhebung der Daten durch das Social Plugin über seine weitergehenden Verarbeitungen zu informieren.[732] Denn

[730] *Golland*, K&R 2019, 533, 535.

[731] Dazu: Kapitel 4 B. III. Fashion ID.

[732] Strenggenommen konnte auch der Websitebetreiber seinen Informationspflichten nicht vor Erhebung der Daten nachkommen, da auch die durch ihn erhobenen Daten bereits beim Öffnen der Webseite erhoben wurden. Für solche Fälle gibt es allerdings mittlerweile Lösungen wie z.B. c't Shariff: *Behr*, https://www.heise.de/hintergrund/Ein-Shariff-fuer-mehr-Datenschutz-2467514.html (abgerufen am 17.07.2024).

auf der Website des Websitebetreibers wurde nur das Social Plugin des Plattformbetreibers angezeigt. Weiterführende Informationen zu dem Social Plugin und den damit verbundenen Verarbeitungen seitens des Plattformbetreibers, die über die des Websitebetreibers hinausgingen, waren gerade nicht möglich. Vergleichbare Szenarien zu diesem sind grundsätzlich immer dann denkbar, wenn Akteure auf fremde Infrastruktur in Form von Soft- oder Hardware zurückgreifen und die Anbieter dieser Infrastruktur nicht direkt mit den betroffenen Personen einer Verarbeitung in Kontakt treten können. Als weiteres Szenario wäre etwa die Verarbeitung von Daten in Smart Cars zwischen Herstellern und den Anbietern von Hard- und Softwarekomponenten vorstellbar. Denn regelmäßig wird nur der Hersteller des Fahrzeugs gegenüber der betroffenen Person in Erscheinung treten.

Ein denkbarer Lösungsansatz für die fehlende Interaktionsmöglichkeit zwischen dem gemeinsam Verantwortlichen, der weitergehende Verarbeitungen vornimmt, und der betroffenen Person wäre, den gemeinsam Verantwortlichen, der die Infrastruktur verwendet, als „Boten" zu nutzen.[733] Dabei müsste allerdings geklärt werden, wie dieser „Bote" unionsrechtlich einheitlich zu bewerten sei. Ein weiterer Lösungsansatz wäre, dass der nur eingeschränkt gemeinsam Verantwortliche dem weitergehend gemeinsam Verantwortlichen die Kontaktdaten der betroffenen Person übermittelt. Diese zusätzliche Verarbeitung würde allerdings offensichtlich das Grundrecht auf Datenschutz gem. Art. 8 GRCh konterkarieren. Sofern eine Möglichkeit der Information der betroffenen Person für den weitergehend gemeinsam Verantwortlichen fehlt, müsste, wenn eine Einwilligung als Verarbeitungsrechtfertigung notwendig ist, jegliche Verarbeitung jenseits der gemeinsam verantworteten Verarbeitungen unterbleiben. Wenn also beispielsweise nur die Übermittlung an den weitergehend gemeinsam Verantwortlichen noch gemeinsam verantwortet wäre, dürfte dieser die Daten zwar empfangen, allerdings nicht speichern und müsste sie daher direkt löschen. Soweit andere Verarbeitungsrechtfertigungen neben der Einwilligung bestünden, wäre als Sanktion der nicht befolgten Informationspflichten nur ein Schadensersatz gegenüber der betroffenen Person bzw. eine Geldbuße seitens der Aufsichtsbehörde möglich. Als Konsequenz nicht befolgter Informationspflichten dürfte es zudem denkbar, letztlich aber fernliegend sein, im Rahmen der Verarbeitungsrechtfertigung des berechtigten Interesses gem. Art. 6 Abs. 1 lit. f DSGVO das Abwägungsergebnis zulasten des Verantwortlichen zu modifizieren. Nach ErwGr 47 S. 3 und 4 DSGVO ist zwar der vernünftige Erwartungshorizont der betroffenen Person für diese Abwägung relevant. Damit dürfte aber

[733] Vgl. *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 69 f., 94 ff.

eine individualisierte Sozialadäquanz gemeint sein und nicht eine Rückkopplung der Informationspflichten auf die Verarbeitungsrechtfertigung erfolgen.

Verwunderlich ist in Anbetracht des vorgangsorientierten Ansatzes zudem, dass der EuGH im Urteil zu der Rechtssache Fashion ID regelmäßig von einer Erhebung und Übermittlung,[734] teilweise aber auch nur von einem dieser beiden Vorgänge spricht.[735] Der EuGH legt zwar besonderen Wert auf den individuellen Vorgang, scheitert aber selbst am Anspruch sauber zwischen den Vorgängen zu differenzieren.[736]

Festhalten lässt sich insgesamt, dass der vorgangsorientierte Ansatz zwar ein brauchbarer Ansatz dafür ist, die Reichweite der gemeinsamen Verantwortlichkeit klarer einzugrenzen,[737] allerdings führt er auch zu Folgeproblemen hinsichtlich der Transparenz der Verarbeitung sowie bei den Pflichten des Verantwortlichen.

2. Anteil oder Verhältnis der Verantwortlichkeit

Neben der Erwähnung des Grades der Verantwortlichkeit weist der EuGH im Urteil zu der Rechtssache Fashion ID darauf hin, dass „[...] die Verantwortlichkeit des Betreibers einer Website [...] noch höher [erscheint], da das bloße Aufrufen einer solchen Website, die den „Gefällt mir"-Button von Facebook enthält, offenbar automatisch die Verarbeitung ihrer personenbezogenen Daten durch Facebook Ireland auslöst."[738] Neben der bereits erörterten Reichweite der individuellen Verantwortlichkeit eines gemeinsam Verantwortlichen scheint es also auch noch eine andere Dimension der Verantwortlichkeit zu geben.[739] Um einer Verwechslung mit dem vom EuGH bemühten Begriffs des Grades der Verantwortlichkeit vorzugreifen, kann man hier vom Anteil an der Verantwortlichkeit oder dem Verhältnis der Verantwortlichkeit der gemeinsam Verantwortlichen untereinander sprechen.

---

[734] Vgl. zum technischen Hintergrund bei der Einbindung von Drittinhalten *Moos*, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible (Hrsg.), Der Schutz der Persönlichkeit im Internet, 2012, 147 ff.

[735] So nur „übermitteln" in Rn. 26, 27, 34, 64. In Rn. 80 hingegen Erheben und Übermitteln.

[736] Kritisch: *Moos/Rothkegel*, MMR 2019, 584, 585. Mit schwammiger Rechtfertigung: *Golland*, K&R 2019, 533, 535. Vgl. *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 7.

[737] So etwa *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 67 ff.: „[...] das entscheidende Puzzlestück [...]".

[738] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 83.

[739] Vgl. die Abgrenzung bei S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 50 im Hinblick auf den Innenregress und die Geldbußen.

a) Notwendigkeit der Feststellung des Verhältnisses?

Zunächst ist fraglich, wozu die Feststellung eines Verhältnisses der Verantwortlichkeit dient.[740] Nach Art. 26 Abs. 3 DSGVO und Art. 82 Abs. 4 DSGVO ist eine Feststellung des Verhältnisses der jeweiligen Verantwortlichkeit der gemeinsam Verantwortlichen für die betroffene Person im Rahmen der Betroffenenrechte und des Schadensersatzes nicht erforderlich. Gegenüber der betroffenen Person besteht eine Art „Gesamtverantwortlichkeit" nach Art. 26 Abs. 3 DSGVO sowie eine Gesamtschuld nach Art. 82 Abs. 4 DSGVO.[741]

Allerdings werden gem. Art. 26 Abs. 3 DSGVO nur die betroffenen Personen hinsichtlich ihrer Rechte privilegiert.[742] Die Aufsichtsbehörden sind also nicht gleichermaßen schutzbedürftig.[743] Daher findet sich auch keine Entsprechung für Art. 26 Abs. 3 DSGVO in den Abhilfebefugnissen in Art. 58 DSGVO. Abseits einer solchen Norm für Aufsichtsbehörden muss für die Frage, welcher gemeinsam Verantwortliche welche Pflicht erfüllt, zunächst auf den Inhalt der Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO zurückgegriffen werden. Ein Rückgriff auf die Vereinbarung kann aber nur dann erfolgen, wenn die gemeinsam Verantwortlichen die maßgebliche Pflicht überhaupt intern verteilt haben und eine Vereinbarung vorliegt.[744] Ist dies nicht der Fall, spricht nichts dagegen, alle oder jedenfalls einen der gemeinsam Verantwortlichen aufsichtsbehördlich zu belangen,[745] ohne vorher das jeweilige Verhältnis der Verantwortlichkeit zu ermitteln.[746] Wäre in Ermangelung einer Vereinbarung nach Art. 26 Abs.1 S. 2 DSGVO eine Feststellung des jeweiligen Verhältnisses der Verantwortlichkeit für die Ergreifung von Abhilfemaßnahmen notwendig, fehlt es an einem Anreiz für gemeinsam Verantwortliche, diese Vereinbarung überhaupt abzuschließen. Selbst bei Feststellung eines bestimmten Verhältnisses der Verantwortlichkeit lässt sich daraus

[740] Vgl. *Kollmar*, NVwZ 2019, 1740, 1742. Abgesehen von der Machbarkeit: *Augsberg*, RW 2019, 109, 115.

[741] Überholt erscheint mit diesen Normen die Ansicht der Art. 29-Datenschutzgruppe, dass nicht in allen Formen gemeinsam Verantwortlicher eine Gesamtschuld vorliegt (*Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 39): *Hacker*, MMR 2018, 779, 780.

[742] Sydow/Marsch/*Ingold*, Art. 26 DSGVO, Rn. 10; Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 109. Vgl. zur Schwierigkeit der Geltendmachung eines Schadensersatzes ggü. Verantwortlichen allein aufgrund der Problematik der Feststellung des Verantwortlichen *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 10 ff.

[743] *Schreiber*, ZD 2019, 55, 58.

[744] Vgl. *Bock*, K&R 2019, 30, 32; *Gierschmann*, ZD 2020, 69, 69; *Söbbing*, ITRB 2020, 218, 219.

[745] Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 109. Vgl. zu einer Stufenfolge im Hinblick auf die Adressatenauswahl für das BDSG a.F. BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 19.

[746] Dazu: Kapitel 4 L. VI. Störerauswahl bei aufsichtsbehördlichen Maßnahmen.

nicht auf die konkreten Pflichten eines individuellen gemeinsam Verantwortlichen schließen. Bei allen nicht paritätisch verteilten Verhältnissen der Verantwortlichkeit würde naheliegenderweise immer der Verantwortliche mit dem höchsten Verhältnis von den Aufsichtsbehörden belangt werden. Gegen eine grundsätzliche Pflicht der Aufsichtsbehörden zur Ermittlung des Verhältnisses der Verantwortlichkeit spricht zudem, dass nach Art. 26 Abs. 1 S. 2 DSGVO die Vereinbarung zwischen den gemeinsam Verantwortlichen nicht nur auf Betroffenenrechte beschränkt ist.[747] Die gemeinsam Verantwortlichen können also auch eine Verteilung der Pflichten jenseits der Betroffenenrechten gegenüber der Aufsichtsbehörde im Rahmen der Vereinbarung klarstellen.[748] Weiterhin kann die Aufsichtsbehörde im Rahmen der Beschwerde nach Art. 77 Abs. 1 DSGVO für betroffene Personen tätig werden. Warum mit dem Umweg über die vermeintlich kompetente Aufsichtsbehörde der betroffenen Person die Durchsetzung ihrer Rechte durch die Notwendigkeit der Feststellung des Verhältnisses der Verantwortlichkeit wieder erschwert werden soll, erschließt sich also nicht.[749]

Zwar müssen Maßnahmen nach Art. 58 DSGVO gem. ErwGr 129 S. 5 DSGVO verhältnismäßig sein.[750] Allerdings bezieht sich diese Verhältnismäßigkeit auf die Maßnahme selbst.[751] Für die Auswahl des Adressaten einer Maßnahme gilt dies aufgrund des Grundsatzes der Effektivität der Maßnahme nur eingeschränkt.[752] Das Verhältnis der Verantwortlichkeit als Aspekt der Verhältnismäßigkeit wäre also allenfalls eingeschränkt zu berücksichtigen, etwa in offensichtlichen Fällen. Auch der Einwand, der Aufsichtsbehörde stünden doch die Untersuchungsbefugnisse gem. Art. 58 Abs. 1 DSGVO zur Verfügung, geht fehl.[753] Die Untersuchungsbefugnisse bestehen selbst bei singulär Verantwortlichen, etwa um festzustellen, ob überhaupt eine Verantwortlichkeit vorliegt. Es ließe sich umgekehrt argumentieren, dass der singulär Verantwortliche benachteiligt wäre, wenn bei gemeinsam Verantwortlichen erhöhte Untersuchungsanforderungen für die Aufsichtsbehörde bestehen würden.

---

[747] Der Wortlaut „insbesondere" macht deutlich, dass die Auflistung nicht abschließend ist.

[748] A.A.: *Schreiber*, ZD 2019, 55, 58.

[749] Vgl. *Roßnagel*, MMR 2005, 71, 75 zur Institutionalisierung der Kontrolle. Insgesamt zur Funktion der Aufsichtsbehörde: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 37.

[750] So: *Schreiber*, ZD 2019, 55, 59.

[751] Für das BDSG a.F. hatte BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 19 festgestellt, dass die ermessensgerechte Adressatenauswahl der Maßnahme selbst ggü. vorverlagert ist.

[752] BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 30. Ausnahmen vom Verhältnismäßigkeitsgrundsatz gelten etwa bei fehlender Eignung der Maßnahme gegenüber einem bestimmten Adressaten: ebd., Rn. 18 (noch zur Rechtslage BDSG a.F.). Umgekehrt beeinflusst die Auswahl des Adressaten auch die Maßnahme, sofern es nicht nur um die Duldung der Maßnahme im Innenverhältnis geht, vgl. *Schreiber*, ZD 2019, 55, 60.

[753] Siehe: *Schreiber*, ZD 2019, 55, 58.

Sofern eine Abhilfebefugnis einen Verantwortlichen verlangt, genügt also auch ein hinsichtlich des Verhältnisses der Verantwortlichkeit nur geringfügig gemeinsam Verantwortlicher. Soweit sich das Innenverhältnis der gemeinsam Verantwortlichen nicht offensichtlich nach außen manifestiert,[754] kann die Aufsichtsbehörde Untersuchungen zum Verhältnis der Verantwortlichkeit der gemeinsam Verantwortlichen grundsätzlich unterlassen. Zwar sollte die Aufsichtsbehörde im Gegensatz zur betroffenen Person auch Kriterien wie einen Ermöglichungs- oder Verschuldensbeitrag des individuellen gemeinsam Verantwortlichen berücksichtigen. Das gilt aber nur, soweit dies unter dem Primat der Effektivität der Gefahrenabwehr möglich ist.[755]

Etwas anderes gilt für die durch die Aufsichtsbehörde verhängten Geldbußen nach Art. 58 Abs. 2 lit. i i.V.m. 83 DSGVO. Für Geldbußen gibt es keine Art. 82 Abs. 4 DSGVO entsprechende Norm, die eine Gesamtschuld anordnet. Geldbußen werden also nicht gemeinsam Verantwortlichen kollektiv auferlegt, sondern immer nur individuellen gemeinsam Verantwortlichen. Daher ist hinsichtlich der Geldbußen notwendigerweise das Verhältnis der Verantwortlichkeit zu bestimmen. Bei den Geldbußen nach Art. 83 Abs. 1 DSGVO gilt zudem der Grundsatz der Verhältnismäßigkeit unmittelbar.[756] Daneben erwähnt Art. 83 Abs. 2 lit. d DSGVO explizit den Grad[757] der Verantwortung für die Entscheidung über die Verhängung einer Geldbuße und deren Betrag.[758] Dabei sind Einflussmöglichkeiten des individuellen gemeinsam Verantwortlichen wie auch die tatsächliche Aufgabenwahrnehmung nach Art. 26 Abs. 1 S. 2 DSGVO relevant.[759] Daher ist eine genauere Analyse des Einzelfalls notwendig. Bis auf die Geldbußen ist im Außenverhältnis das Verhältnis der Verantwortlichkeit eines gemeinsam Verantwortlichen hingegen grundsätzlich irrelevant.[760]

Insgesamt ist die Feststellung des Verhältnisses der Verantwortlichkeit für die Bemessung einer Geldbuße[761] nach Art. 83 Abs. 2 S. 2 lit. d DSGVO erforderlich, ferner

[754] Vgl. die „objektive Qualifikation" der Vorgänge bei: *Schreiber*, ZD 2019, 55, 58.

[755] BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 30.

[756] *Schreiber*, ZD 2019, 55, 60.

[757] Dabei scheint die DSGVO den Begriff aber im Sinne des hier vorgeschlagenen Verhältnisses der Verantwortlichkeit zu verstehen.

[758] A. ErwGr 148 S. 2, 3 DSGVO erwähnen die Verhältnismäßigkeit sowie den Grad der Verantwortlichkeit.

[759] So a.: *Schreiber*, ZD 2019, 55, 60.

[760] So jedenfalls für die betroffene Person: Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 29; *Schreiber*, ZD 2019, 55, 58; *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 507. Vgl. a. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 205 mit Fokus auf die Rechtsfolgenseite.

[761] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 69.

potenziell für die Haftungsquote[762] nach Art. 82 Abs. 5 DSGVO.[763] Der Schadenersatz wird bei gemeinsam Verantwortlichen gem. Art. 82 Abs. 4 DSGVO hingegen bereits durch den vorgangsorientierten Ansatz begrenzt.[764] Abseits der Bemessung einer Geldbuße ist der maßgebliche Ort für die Feststellung des Verhältnisses der Verantwortlichkeit also vor allem das Innenverhältnis der gemeinsam Verantwortlichen.[765]

b) Kriterien für das Verhältnis der Verantwortlichkeit

Sofern die Feststellung des Verhältnisses der Verantwortlichkeit notwendig ist, stellt sich zunächst die Frage, für welche Bemessungsgröße das Verhältnis festgestellt wird. Denkbar ist es hier, global auf alle gemeinsam verantworteten Vorgänge abzustellen oder jeweils auf individuelle Vorgänge. Eine globale Feststellung des Verhältnisses der Verantwortlichkeit anhand aller gemeinsam verantworteten Vorgänge stünde allerdings im Widerspruch zum vorgangsorientierten Ansatz des EuGH. Zudem hat der EuGH im Urteil zu der Rechtssache Fashion ID auch explizit festgestellt, dass das Ausmaß der Verantwortlichkeit zwischen verschiedenen Vorgängen durchaus divergieren kann.[766] Aufgrund der individuellen Verarbeitungsvorgänge als Maßstab des Verhältnisses der Verantwortlichkeit kann innerhalb einer gemeinsamen Verantwortlichkeit daher nicht von einer pauschalen Abstufung ausgegangen werden.[767]

Die einzelnen Kriterien für die Feststellung des Verhältnisses der Verantwortlichkeit sind bislang unklar. Der EuGH verlangt ganz allgemein eine Berücksichtigung aller maßgeblichen Umstände des Einzelfalls.[768] Über die tatsächlichen und rechtlichen Einflussmöglichkeiten individueller gemeinsam Verantwortlicher sowie die interne Verteilung der Aufgaben und Pflichten besteht nach außen hin, auch unter Berücksichtigung der Vereinbarung gem. Art. 26 Abs. 1 S. 2 DSGVO, selten Klarheit. Trotzdem dürften

[762] Dazu: Kapitel 3 A. Haftung auf Schadensersatz.
[763] Vgl. *Schreiber*, ZD 2019, 55, 58; *Hanloser*, ZD 2019, 455, 459.
[764] *Kollmar*, NVwZ 2019, 1740, 1742.
[765] So schlägt der EDPS eine Pflichtenverteilung im Innenverhältnis vor: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 26 f.; kritisch zur Möglichkeit in der zunehmend komplexen Informationsverarbeitung: *Augsberg*, RW 2019, 109, 115 f.
[766] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70.
[767] Vgl. *Jung/Hansch*, ZD 2019, 143, 144; anders: *Hanloser*, ZD 2019, 455, 459. Kritisch zur Frage, was damit gewonnen wäre: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 28.
[768] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70.

diese Kriterien, auch nach dem Verständnis der Art. 29-Datenschutzgruppe,[769] ein sinnvoller Ansatzpunkt sein.[770]

Ein denkbares Kriterium für die Feststellung des Verhältnisses der Verantwortlichkeit könnte der Zugang zu den verarbeiteten Daten und das damit erhöhte Missbrauchsrisiko sein. Zwar hat der EuGH im Urteil zu der Rechtssache Fashion ID festgehalten, dass fehlender Zugang zu den verarbeiteten Daten unschädlich für eine gemeinsame Verantwortlichkeit insgesamt ist.[771] Dies sagt allerdings noch nichts darüber aus, ob dies nicht wenigstens ein Kriterium für das Verhältnis der Verantwortlichkeit sein könnte.[772]

Letztlich dürfte es zur Feststellung des Verhältnisses der Verantwortlichkeit auf eine Gesamtschau der Faktoren hinauslaufen, die den Einfluss auf die Zwecke und Mittel der Verarbeitung betreffen, sowie auf die Verteilung der Pflichten zwischen den gemeinsam Verantwortlichen.[773] Zwar kommt den vertraglichen Vereinbarungen der gemeinsam Verantwortlichen hierbei eine Indizwirkung zu, maßgeblich sind allerdings die tatsächlichen Umstände.[774] Dies wird indirekt durch Art. 26 Abs. 2 S. 1 DSGVO bestätigt, der gemeinsam Verantwortliche zum Wahrheitsgehalt der Vereinbarung verpflichtet.

3. Fazit

Ein individueller gemeinsam Verantwortlicher ist nur für die Verarbeitungsvorgänge verantwortlich, für die ein Entscheidungsbeitrag von ihm und dadurch eine von ihm mit verantwortete gemeinsame Entscheidung vorliegt. Er ist nicht für vor- oder nachgelagerte Verarbeitungsvorgänge anderer gemeinsam Verantwortlicher verantwortlich, für die er keinen Entscheidungsbeitrag leistet. Abseits der Bemessung einer Geldbuße ist sein Verhältnis der Verantwortlichkeit grundsätzlich nur im Innenverhältnis der gemeinsam Verantwortlichen relevant.

---

[769] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 12, ebenso: *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 138 ff.

[770] Vgl. *Schreiber*, ZD 2019, 55, 58.

[771] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 69.

[772] So etwa: *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 24; ebenso: *Cimina*, ERA Forum 2020, 7.

[773] Eine oberflächliche Auflistung findet sich bei: *Schreiber*, ZD 2019, 55, 58.

[774] So a.: *Schreiber*, ZD 2019, 55, 58.

III. Art. 26 Abs. 3 DSGVO als „gesamtschuldnerische Verantwortlichkeit"?

Im Zusammenhang mit der autonomen Erfüllungsfähigkeit sowie der Delegation von Pflichten[775] zwischen gemeinsam Verantwortlichen stellt sich zunächst die Frage, ob Art. 26 Abs. 3 DSGVO eine Art „gesamtschuldnerische Verantwortlichkeit" der gemeinsam Verantwortlichen für die Erfüllung der Betroffenenrechte anordnet.[776] Sofern Art. 26 Abs. 3 DSGVO eine solche „gesamtschuldnerische Verantwortlichkeit" anordnen sollte, bestünde im Umkehrschluss die Notwendigkeit einer autonomen Erfüllungsfähigkeit der Pflichten durch die individuellen gemeinsam Verantwortlichen.[777] Dies wiederum würde die Möglichkeit der Delegation[778] von Pflichten zwischen gemeinsam Verantwortlichen faktisch verhindern. Der Anwendungsbereich der gemeinsamen Verantwortlichkeit wäre durch eine solche „gesamtschuldnerische Verantwortlichkeit" also stark eingeschränkt.

Auch wenn Art. 26 Abs. 3 DSGVO eine der Gesamtschuld vergleichbare Wirkung für die Wahrnehmung der Rechte der betroffenen Person auf der Kontaktebene entfaltet,[779] ihr nämlich die Wahlfreiheit hinsichtlich des Ansprechpartners zugesteht, handelt es sich bei der Norm nicht um die Anordnung einer (Art) Gesamtschuld.[780] Dies wird nicht zuletzt dadurch deutlich, dass der Unionsgesetzgeber in Art. 82 Abs. 4 DSGVO die Worte „[...] so haftet jeder Verantwortliche [...] für den gesamten Schaden [...]" verwendet, während er in Art. 26 Abs. 3 DSGVO vorgibt, dass „[...] die betroffene Person ihre Rechte [...] bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen [kann]".[781] Die Position des Europäischen Parlaments im Gesetzgebungsverfahren zu Art. 26 DSGVO[782] enthielt dagegen noch die explizite Formulierung: „Im Fall unklarer Verantwortlichkeiten haften die für die Verarbeitung Verantwortlichen

[775] Dazu die nächsten beiden Unterkapitel.

[776] So etwa: *Monreal*, CR 2019, 797, Rn. 1; Sydow/Marsch/*Ingold*, Art. 26 DSGVO, Rn. 10; Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, 29.

[777] Dazu: Kapitel 4 L. IV. Autonome Erfüllungsfähigkeit von Pflichten?

[778] Dazu: Kapitel 4 L. V. Delegation von Pflichten zwischen gemeinsam Verantwortlichen.

[779] Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 36; *Hacker*, MMR 2018, 779, 780; *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 104.

[780] „Keine originäre gemeinsame Erfüllungsverantwortung" Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 40; ebd., Rn. 14; skeptisch: Kühling/Buchner/*Hartung*, Art. 26 DS-GVO, Rn. 64. Die Art. 29-Datenschutzgruppe setzt in WP 169 gesamtschuldnerisch in Anführungszeichen: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 39. Simitis/Hornung/Spiecker/*Petri*, Art. 26 DSGVO, Rn. 28 spricht von einer Vergleichbarkeit zur Gesamtschuld.

[781] Vgl. die Erwägungen bei *Augsberg*, RW 2019, 109, 116 zum Zurechnungsendpunkt.

[782] Entsprechend Art. 24 DSGVO-KOM-E.

gesamtschuldnerisch."[783] Es erscheint also bereits aufgrund des finalen Wortlauts der DSGVO kaum zielführend, die Geltendmachung und die Gesamtschuld begrifflich zu vermischen.[784] Unter Umständen kann derjenige gemeinsam Verantwortliche, bei dem die betroffene Person ihre Rechte geltend macht, diesen Rechten gar nicht nachkommen und muss die Erfüllung einer Pflicht an die anderen gemeinsam Verantwortlichen delegieren oder jedenfalls versuchen, auf diese entsprechend einzuwirken.[785]

Nach einem engen (deutschen) zivilrechtlichen Verständnis der Haftung wäre bei fehlender Erfüllungsmöglichkeit dieses gemeinsam Verantwortlichen dann aber die Erfüllung eines Betroffenenrechts, als Anspruch verstanden, unmöglich und die betroffene Person hätte hinsichtlich der Durchsetzung ihrer Ansprüche nichts gewonnen.[786] Ein solches Ergebnis war aber offensichtlich nicht Absicht des Unionsgesetzgebers. Dieser wollte mit Art. 26 Abs. 3 DSGVO vielmehr komplexen und intransparenten Zuständigkeitsszenarien vorbeugen. Es gibt daneben keinen Regress der gemeinsam Verantwortlichen untereinander wegen Über- oder Untererfüllung der Betroffenenrechte, vergleichbar zu Art. 82 Abs. 5 DSGVO. Auch passt bereits der Wortlaut von § 421 BGB, also für die (deutsche) zivilrechtliche Gesamtschuld, nicht auf die Betroffenenrechte.[787] Die betroffene Person kann, verstanden als Gläubiger, ihre Betroffenenrechte gegenüber allen gemeinsam Verantwortlichen gleichzeitig geltend machen und ist nicht auf die einmalige Geltendmachung gegenüber einem individuellen gemeinsam Verantwortlichen beschränkt. Daneben ist schlicht nicht vorstellbar, wie etwa ein Auskunftsrecht. nur teilweise durch einen gemeinsam Verantwortlichen erbracht werden sollte. Beim Schadensersatz nach Art. 82 Abs. 4 DSGVO hingegen lässt sich der Rechtsgedanke von § 421 BGB unproblematisch übertragen.

Der Begriff der Haftung bezeichnet im deutschen Recht üblicherweise das Einstehenmüssen für eine aus einem Schuldverhältnis herrührende Schuld, in einem engeren Sinn die Haftung des Vermögens des Schuldners gegenüber dem Zugriff des Gläubigers.[788] Dies deckt sich mit dem unionsrechtlichen Verständnis der Haftung, etwa der Staatshaftung aus Art. 340 AEUV. Die Haftung (nach deutschem Verständnis) aus dem Vermögen setzt allerdings regelmäßig ein Verschulden einer Partei im Hinblick

[783] Art. 24 EP-PE_TC1-COD(2012)0011. Vgl. a. Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 4.
[784] Vgl. *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 30 Fn. 46.
[785] Vgl. *Cimina*, ERA Forum 2020, 10; Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 103 f. In diese Richtung: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 86.
[786] Ob gemeinsam Verantwortliche regelmäßig Erfüllungs- oder Verrichtungsgehilfen wären, ist zweifelhaft.
[787] Inwiefern ein unionsrechtliches Verständnis der Gesamtschuld hiervon abweicht, sei dahingestellt.
[788] *Weber*, Rechtswörterbuch, [24]2022, 792 f.

auf eine Pflichtverletzung voraus.[789] Die polizei- bzw. ordnungsrechtliche Verantwortlichkeit (nach deutschem Verständnis) hingegen setzt gerade kein Verschulden voraus.[790] Mit dem eben beschriebenen Verständnis von Haftung wären Pflichten aus der DSGVO oder die aufsichtsbehördlichen Maßnahmen also nicht erfasst. Der Begriff Verantwortlichkeit oder präziser des Verantwortlichen entspricht diesbezüglich eher dem Begriff des Störers.[791] Auch in der englischen Rechtssprache scheint, jedenfalls teilweise, eine Unterscheidung zwischen „responsibility" und „liability" vorgenommen zu werden.[792] So sei die Einhaltung der datenschutzrechtlichen Vorgaben im Rahmen der Verantwortlichkeit die Voraussetzung am (datenschutzrechtlich relevanten) Geschäftsleben teilzunehmen.[793] Die Verantwortlichkeit ist demnach eine der Haftung vorgelagerte Frage im Datenschutzrecht. Folglich sind Verantwortlichkeit und Haftung also nicht identisch.

Aufgrund der hybriden Durchsetzungsnatur des Datenschutzrechts, zum einen direkt anhand der Betroffenenrechte, zum anderen durch die Aufsichtsbehörden, ergibt es wenig Sinn, der DSGVO ein starres (deutsches) zivilrechtliches „Korsett" überzustülpen.[794] Die Pflicht, den Betroffenenrechten nachzukommen erwächst allein aus der Stellung als Verantwortlicher. Der Begriff der Haftung taucht in der DSGVO schließlich nur im Rahmen des Schadensersatzes nach Art. 82 auf. Er setzt seinerseits wiederum eine Verantwortlichkeit oder Auftragsverarbeitung voraus.[795] Die gesamtschuldnerische Haftung nach Art. 82 Abs. 4 DSGVO setzt zudem, in weiterer Abgrenzung zu

[789] Dies gilt etwa nicht für die Gefährdungshaftung.

[790] *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 88, 111, 121, 123; *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 257.

[791] *Weber*, Rechtswörterbuch, [24]2022, 1549 f.; vgl. zu Verantwortlichkeit ebd., 1711.

[792] *Jay*, 17. Administrative Fines and Penalties, in: Jay (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition), 2017, Rn. 17-012, 17-025; *Jay*, 15. Complaints and Judicial Remedies, in: Jay (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition), 2017, Rn. 15–26. A. die englische Version von *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010 differenziert zwischen „responsibility" und „liability". Anders wohl *Ausloos*, The Right To Erasure, 2018, 69 ff., der es als eine Art Leitprinzip versteht. Das von ihm beschriebene Leitprinzip wiederum klingt eher nach dem Accountability-Prinzip aus Art. 5 Abs. 2 DSGVO: *Jay*, 9. Accountability, in: Jay (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition), 2017, Rn. 9-007.

[793] In Bezug auf die e-Commerce-RL: *Keller*, BTLJ[33] (2018), 287, 355.

[794] Vgl. a. die Überlegungen zu einer teleologischen Reduktion von Art. 26 Abs. 3 DSGVO bei *Hacker*, MMR 2018, 779, 783 f.

[795] Vgl. a. die Verbindung zwischen Verantwortlichkeit und Haftung bei S/J/T/K/*Kremer*, Art. 26

Art. 26 Abs. 3 DSGVO, nicht unbedingt gemeinsam Verantwortliche voraus.[796] Wären der Verantwortliche und der Haftende austauschbare Begriffe, wäre Art. 82 Abs. 4 DSGVO gar nicht vonnöten. Dies gilt umso mehr, weil Art. 82 Abs. 1 DSGVO einen Verstoß gegen die DSGVO durch den Verantwortlichen oder Auftragsverarbeiter verlangt, aus dem einer Person ein Schaden entsteht. Schließlich trennt auch ErwGr 74 DSGVO zwischen Verantwortung und Haftung.

Insofern ist es nötig, zwischen dem Begriff der Verantwortlichkeit und der Haftung sauber zu trennen.[797] Denn das Konzept des Verantwortlichen dient primär dazu, einer Stelle die Einhaltung der datenschutzrechtlichen Vorgaben aufzugeben.[798] Auch die Art. 29-Datenschutzgruppe trennt die Konzepte Verantwortlichkeit und Haftung.[799] So sieht sie die zivilrechtliche Haftung ebenso wie Sanktionen als reaktive Mittel, um die Einhaltung der datenschutzrechtlichen Vorgaben, also der Pflichten, durch den Verantwortlichen sicherzustellen.[800] Umgekehrt könne aus allgemeinen gesetzlichen Bestimmungen oder geltender Rechtspraxis, unter anderem aufgrund der zivilrechtlichen Haftung, aber auch teilweise auf die Verantwortlichkeit geschlossen werden.[801] Dabei seien beide Begriffe allerdings nicht austauschbar.[802]

DSGVO, Rn. 87 ff. Zum Begriff „verantwortlich“ in Art. 82 Abs. 3 DSGVO: BeckOK DatenschutzR[47]/*Quaas*, Art. 82 DSGVO, Rn. 17, 17.2.

[796] Vgl. Sydow/Marsch/*Kreße*, Art. 82 DSGVO, Rn. 22. Zu potenziellen Anwendungsfällen: *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 30.

[797] Vgl. *Augsberg*, RW 2019, 109, 110. Zur Verwendung der Begriffe in der EuGH-Rechtsprechung: Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR Update Mai 2021, 38 Fn. 8.

[798] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 6.

[799] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 19 ff.

[800] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 6; ebenso: *Alsenoy*, CLSR[28] (2012), 25, 29.

[801] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 13, 19.

[802] „Wie bereits erläutert, ist die Rolle des für die Verarbeitung Verantwortlichen für die Feststellung der Haftung und die Verhängung von Sanktionen von entscheidender Bedeutung.“ *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20.

IV. Autonome Erfüllungsfähigkeit von Pflichten?

Im Verarbeitungsalltag liegt es nahe, dass insbesondere dann eine Zusammenarbeit verschiedener Akteure notwendig ist, wenn ein Akteur nicht im Stande ist, bestimmte Prozesse oder Aufgaben autonom durchzuführen.[803] Diese fehlende Möglichkeit der autonomen Durchführung einer Verarbeitung kann etwa durch mangelnde Infrastruktur, Daten oder auch Expertise bedingt sein. In solchen Szenarien ist nicht immer eine Auftragsverarbeitung, etwa wegen der Voraussetzung einer Weisungsgebundenheit, zwischen den Akteuren möglich. Sofern bestimmte Verarbeitungsvorgänge zwischen gemeinsam Verantwortlichen aufgeteilt werden, führt dies dann regelmäßig dazu, dass nicht alle individuellen gemeinsam Verantwortlichen auch alle materiellrechtlichen Pflichten der DSGVO autonom erfüllen können.[804] Dies gilt insbesondere für die Betroffenenrechte. Denkbar wäre es, die Verantwortlichkeit derjenigen Akteure, die nicht alle ihre Pflichten aus der DSGVO autonom erfüllen können, generell abzulehnen. Dies würde dazu führen, dass solche Akteure zwar tatbestandlich gemeinsam Verantwortliche darstellen, auf der Erfüllungsebene allerdings wieder aus der gemeinsamen Verantwortlichkeit herausfielen.[805] Fraglich ist aber, ob eine solche autonome Erfüllungsfähigkeit aller Pflichten der DSGVO überhaupt Voraussetzung der gemeinsamen Verantwortlichkeit ist.

1. Rechtsprechung des EuGH und Definition

Der EuGH hat in der Rechtssache Google Spain entschieden: „[...] hat der Suchmaschinenbetreiber daher in seinem Verantwortungsbereich **im Rahmen seiner Befugnisse und Möglichkeiten** dafür zu sorgen, dass die Tätigkeit den Anforderungen der RL 95/46/EG entspricht [...]."[806] Dies lässt sich so interpretieren, dass eine gewisse Flexibilität für spezifische Pflichten eines Verantwortlichen besteht. Hinsichtlich des Schwerpunktes des Urteils in der Rechtssache Google Spain könnte dies etwa eine nur reaktive Bearbeitung der „Recht auf Vergessen(werden)"-Anträge bedeuten.[807] Dem-

[803] Vgl. zur Erfüllung der Informationspflichten *Monreal*, CR 2019, 797, Rn. 57.

[804] Vgl. a. *European Data Protection Supervisor*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 07.11.2019, 30.

[805] So anscheinend frühere Auffassungen zum BDSG a.F.: *Alich/Nolte*, CR 2011, 741, 743.

[806] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 38 (Hervorhebung durch den Autor).

[807] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 18. Dies führt de facto zu einer Host-Provider Privilegierung nach Art. 6 Abs. 1 DSA.

nach könnten also Pflichten der DSGVO insgesamt aufgrund der Umstände der Verarbeitung eingeschränkt sein und nicht nur von der Erfüllung durch einen individuellen gemeinsam Verantwortlichen abhängen.

Die Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit scheint aber eher gegen ein solch flexibles Verständnis der Pflichten an sich zu sprechen. So hat der EuGH im Urteil zu der Rechtssache Jehovan todistajat[808] festgehalten, dass ein Zugang zu den personenbezogenen Daten – der ja für die Erfüllung vieler Betroffenenrechte elementar ist – nicht durch alle gemeinsam Verantwortlichen notwendig sei.[809] Zumindest ein gemeinsam Verantwortlicher oder gegebenenfalls dessen Auftragsverarbeiter müsse aber Zugang zu den Daten haben. Zwar unterliegt nach der Rechtsprechung des EuGH jeder der gemeinsam Verantwortlichen den datenschutzrechtlichen Vorschriften,[810] dies bedeutet allerdings nicht, dass auch jeder der gemeinsam Verantwortlichen alle diese Vorschriften autonom erfüllen können muss. Dies gilt im Urteil zu der Rechtssache Fashion ID etwa für die rechtzeitige Einholung der Einwilligung der Besucher einer Website durch den Websitebetreiber, auch gegenüber dem Plattformbetreiber.[811] Der Plattformbetreiber muss also die Einwilligung nicht notwendigerweise selbst einholen, die Pflicht zur Einholung einer Einwilligung besteht für ihn aber nichtsdestotrotz. Gerade in Szenarien mit mehreren Verantwortlichen ist also nicht ersichtlich, warum für einen gemeinsam Verantwortlichen bestimmte Pflichten aus der DSGVO eingeschränkt sein oder komplett entfallen sollten, wenn er sich zur Erfüllung dieser Pflichten eines anderen gemeinsam Verantwortlichen bedienen kann.

Auch die Definition der gemeinsam Verantwortlichen lässt keine Notwendigkeit erkennen, dass alle materiellrechtlichen Pflichten autonom erfüllt werden können müssen. Ein gleichwertiger oder unbeschränkter Einfluss auf eine Verarbeitung wird gerade nicht vorausgesetzt. Sinnvoll erscheint demnach eine Unterscheidung zwischen rechtlicher und operativer Kontrolle über die Verarbeitung.[812]

2. Position der Aufsichtsbehörden

Die Art. 29-Datenschutzgruppe hatte bereits in WP 169 festgestellt, dass die Unfähigkeit alle Verpflichtungen eines Verantwortlichen direkt selbst zu erfüllen – etwa das

[808] Dazu: Kapitel 4 B. II. Jehovan todistajat.
[809] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 69.
[810] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 67.
[811] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102.
[812] Siehe: *Alsenoy*, CLSR[28] (2012), 25, 33.

Recht auf Information oder Auskunft –, insbesondere bei gemeinsam Verantwortlichen, die Einstufung als Verantwortlicher nicht verhindere.[813] Zwar sei der Verantwortliche in jedem Fall an seine Verpflichtungen gebunden und dafür haftbar. Die Erfüllung könne aber auch durch andere, die ein engeres Verhältnis mit der betroffenen Person hätten, etwa im Auftrag, erfolgen. Dieses Verständnis deckt sich mit dem Wortlaut aus Art. 26 Abs. 3 DSGVO. Denn diese Norm sieht nur eine Geltendmachung der Betroffenenrechte bei jedem der gemeinsam Verantwortlichen vor, aber nicht notwendigerweise die Erfüllung durch jeden der gemeinsam Verantwortlichen. Bereits vor dem Urteil des EuGH in der Rechtssache Jehovan todistajat ging die Art. 29-Datenschutzgruppe zudem davon aus, dass der Zugriff auf die personenbezogenen Daten keine wesentliche Bedeutung für die Einstufung als Verantwortlicher habe.[814] Insofern kann man hier ein Aufgreifen der Maßstäbe aus dem WP 169 durch den EuGH, auch ohne direkte Bezugnahme, erkennen.

3. Erfüllungsunfähigkeit im Innenverhältnis

Sofern man davon ausgeht, dass eine fehlende autonome Erfüllungsfähigkeit aller materiellrechtlichen Pflichten eines Verantwortlichen nicht die Verantwortlichkeit eines gemeinsam Verantwortlichen überhaupt entfallen lässt, bleibt fraglich, wie bei einer solch einseitigen Unfähigkeit die Pflichten dieses Verantwortlichen zu erfüllen sind. In jedem Fall muss derjenige gemeinsam Verantwortliche, dem die Erfüllung der Pflichten selbst nicht möglich ist,[815] auf den oder die anderen gemeinsam Verantwortlichen hinwirken, die Pflichten zu erfüllen.[816] Für einen Anspruch seitens der betroffenen Person gegenüber einem gemeinsam Verantwortlichen auf ein solches Hinwirken ist nicht unbedingt eine teleologische Reduktion von Art. 26 Abs. 3 DSGVO notwendig, da der Wortlaut ohnehin nur eine Geltendmachung bei jedem der gemeinsam Verantwortlichen vorsieht.[817] Ungeachtet des Erfolgs eines solchen Hinwirkens lässt sich die Recht-

[813] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 27.

[814] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 27.

[815] *Hacker*, MMR 2018, 779, 780 koppelt die Unmöglichkeit bereits an die fehlende Entscheidungsgewalt über einen Umstand der Verarbeitung. Dies dürfte regelmäßig, allerdings nicht zwingend der Fall sein.

[816] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 56; so a. *Hacker*, MMR 2018, 779, 780 mit Verweis auf die BGH-Rechtsprechung zur Störerhaftung: BGH, Urteil vom 28.07.2015 – VI ZR 340/14 = MMR 2016, 210, 39 f.

[817] Vgl. *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 61; *Kollmar*, NVwZ 2019, 1740, 1742. Anders: *Hacker*, MMR 2018, 779, 780.

sprechung des EuGH so verstehen, dass die Auswahl von Dienstleistern, die sich datenschutzwidrig verhalten, ein Haftungsrisiko darstellt und dass durch die Verantwortlichkeit der Nutzer solcher Dienstleister indirekt ein ökonomischer Druck auf diese Anbieter erzeugt werden soll.[818] Insgesamt obliegt es also dem beschränkt erfüllungsfähigen gemeinsam Verantwortlichen eine sorgfältige Auswahl seiner potenziellen gemeinsam Verantwortlichen zu treffen, um die Erfüllung der materiellrechtlichen Pflichten, die ihm selbst nicht möglich sind, sicherzustellen.[819]

4. Konsequenzen der Erfüllungsunfähigkeit gegenüber Aufsichtsbehörden und betroffenen Personen

Ob der gemeinsam Verantwortliche, dem die Erfüllung bestimmter Pflichten selbst nicht möglich ist, mit Abhilfemaßnahmen der Aufsichtsbehörde gem. Art. 58 Abs. 2 DSGVO oder Geldbußen gem. Art. 83 DSGVO belegt werden kann, liegt im Auswahlermessen der Aufsichtsbehörde. Hierbei ist der Verhältnismäßigkeitsgrundsatz, der über Art. 58 Abs. 4 DSGVO Anwendung findet, zu beachten.[820] Hinsichtlich des Schadensersatzes gem. Art. 82 DSGVO besteht nach Abs. 4 bei mehreren Verantwortlichen ohnehin eine Gesamtschuld. Sofern einer der beteiligten Verantwortlichen auf Schadensersatz in Anspruch genommen wird, besteht nach Art. 82 Abs. 5 DSGVO die Möglichkeit, dass dieser Verantwortliche bei den anderen beteiligten Verantwortlichen Regress nimmt. Interne Umstände der gemeinsam Verantwortlichen, die keine Aufnahme in die Quotenberechnung nach Art. 82 Abs. 2 DSGVO finden, können im Innenverhältnis der Verantwortlichen zusammen mit der Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO vorab zur Berücksichtigung festgelegt werden.[821]

5. Fazit

Insgesamt ist es für das Bestehen einer gemeinsamen Verantwortlichkeit also nicht erforderlich, dass jeder gemeinsam Verantwortliche alle seine Pflichten aus der DSGVO autonom erfüllen können muss.

---

[818] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 52.
[819] *Hacker*, MMR 2018, 779, 780 m.w.N.
[820] Ebenso: ErwGr 129 S. 5 DSGVO; Ehmann/Selmayr/*Selmayr*, Art. 58 DS-GVO, Rn. 6.
[821] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 173.

V. Delegation von Pflichten zwischen gemeinsam Verantwortlichen

Unabhängig von der Frage einer weitergehenden Privilegierung gemeinsam Verantwortlicher können jedenfalls bestimmte Pflichten aus der DSGVO zwischen den gemeinsam Verantwortlichen aufgeteilt werden.[822] Denn Art. 26 Abs. 1 S. 2 DSGVO sieht explizit eine solche Aufteilung vor.[823] Art. 26 Abs. 3 DSGVO steht zu dieser Aufteilung nicht im Widerspruch, da dort nur die Geltendmachung ihrer Rechte durch die betroffene Person, nicht aber die interne Pflicht zu deren Erfüllung zwischen den gemeinsam Verantwortlichen normiert wird.[824] Eine Aufteilung der Pflichten zwischen den gemeinsam Verantwortlichen ist allerdings insoweit begrenzt, wie das Unionsrecht oder das Recht der Mitgliedstaaten Pflichten bestimmten gemeinsam Verantwortlichen zuweist.[825] Die aufgeteilten Pflichten müssen zudem nicht gleichmäßig zwischen den gemeinsam Verantwortlichen verteilt sein.[826] Da Art. 26 Abs. 1 S. 2 DSGVO „insbesondere" von den Betroffenenrechten und den Informationspflichten spricht, können neben diesen Pflichten auch noch weitere Pflichten aufgeteilt werden.[827]

1. Delegationsfähigkeit von Pflichten

Die Aufteilung der Pflichten ist nur für die in Kapitel III – „Rechte der betroffenen Person" (Art. 12 - 23) der DSGVO genannten Pflichten sicher möglich.[828] Neben die-

---

[822] Vgl. zum Inhalt der Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 148 ff.

[823] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 168; Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 26; Sydow/Marsch/*Ingold*, Art. 26 DSGVO, Rn. 8; *Lezzi/Oberlin*, ZD 2018, 398, 402. Im Hinblick auf die Rechtssache Fashion ID (dazu unten) scheint die Anmerkung von *Kremer*, CR 2019, 676, Rn. 26, dass über die Verteilung der Pflichten der gemeinsam Verantwortlichen nicht entschieden wurde, nicht richtig, da eine einseitige Informationspflicht durch den Websitebetreiber (wenn a. in Verbindung mit der Vorbereitung der Einwilligung) durch den EuGH ja festgestellt wurde.

[824] *Hacker*, MMR 2018, 779, 780 möchte Art. 26 Abs. 3 DSGVO hingegen insoweit teleologisch reduzieren, obwohl dafür keine Veranlassung besteht. Inwiefern eine Entscheidungsgewalt im Hinblick auf die konkrete Verpflichtung nicht nur indikativ, sondern maßgeblich für deren Erfüllbarkeit sein soll, erschließt sich daneben a. nicht.

[825] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 162; Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 80; *Lezzi/Oberlin*, ZD 2018, 398, 402. Zum BDSG: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 4.

[826] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 169. Vgl. zur Verteilung auch *Folkerts*, ZD 2022, 201.

[827] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 165.

[828] G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 55 f. erwägt noch Pflichten aus Kapitel IV (Art. 24-43) und V (Art. 44-50).

sen Pflichten dürfte die Möglichkeit zur Aufteilung zwischen gemeinsam Verantwortlichen nur wenige weitere Pflichten betreffen.[829] Für die Feststellung solcher weiteren Pflichten muss zwischen Pflichten, die die Verarbeitung als Bezugspunkt haben, und solchen, die den Verantwortlichen als Bezugspunkt haben, unterschieden werden.[830] Pflichten mit Bezugspunkt zur Verarbeitung dürften grundsätzlich eher zwischen den gemeinsam Verantwortlichen verteilt werden können als solche, die den Verantwortlichen als Bezugspunkt haben. Bei Pflichten, die den Verantwortlichen selbst als Bezugspunkt haben, muss überprüft werden, inwiefern eine Aufteilung zwischen den gemeinsam Verantwortlichen sinnvoll durchführbar ist.[831] Abwegig wäre die Aufteilung beispielsweise bei der Pflicht gem. Art. 27 DSGVO einen Vertreter oder gem. Art. 37 DSGVO einen Datenschutzbeauftragten zu bestellen. Auch die Vorgaben zum Verarbeitungsverzeichnis gem. Art. 30 DSGVO zeigen, dass jeder Verantwortliche ein solches selbst führen muss.[832] Bei Pflichten wie der Sicherheit der Verarbeitung gem. Art. 32 DSGVO oder der Durchführung einer Datenschutzfolgeabschätzung gem. Art. 35 DSGVO scheint eine Aufteilung dagegen unproblematischer.[833]

2. Konsequenz des Fehlens einer Vereinbarung

Unklar ist, ob und wie eine Aufteilung der Pflichten erfolgt, wenn die gemeinsam Verantwortlichen entgegen Art. 26 Abs. 1 S. 2 DSGVO keine Vereinbarung abgeschlossen haben.[834] In diesem Fall musste nach Ansicht der Art. 29-Datenschutzgruppe die Aufteilung der individuellen Pflichten anhand der tatsächlichen Umstände erfolgen. Falls dies nicht möglich wäre, seien alle gemeinsam Verantwortlichen (quasi) gesamtschuldnerisch verantwortlich.[835] Der EDPB hat hinsichtlich der DSGVO zu dieser Frage keine

[829] Eine Auflistung von potenziell delegierbaren Pflichten findet sich bei: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 166.; Vgl. a. *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 154 ff.; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 258 ff.; *Schreiber*, ZD 2019, 55, 57.

[830] Ähnlich: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 76 f.

[831] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 169; siehe a.: *Lezzi/Oberlin*, ZD 2018, 398, 402.

[832] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 170; siehe a.: Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 27; *Bock*, K&R 2019, 30, 32. Ein gemeinsam erstelltes Verarbeitungsverzeichnis kann aufgrund des gemeinsamen Wissenspools über die Verarbeitungen dennoch sinnvoll sein.

[833] So a.: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 166.

[834] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 50, 67.

[835] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 29 f.

Stellung bezogen. Die Auffassung der Art. 29-Datenschutzgruppe ist konsequent. Denn eine fehlende Vereinbarung geht zu Lasten der gemeinsam Verantwortlichen. Fehlt eine Vereinbarung gem. Art. 26 Abs. 1 S. 2 DSGVO, auch nur zur Aufteilung der Pflichten, führt dies zwar zu einer Rechtswidrigkeit der Verarbeitung[836] sowie potenziell zu einer Geldbuße gem. Art. 83 Abs. 4 lit. a DSGVO.[837] Dies lässt aber die Verarbeitungsrechtfertigung aus Art. 6 Abs. 1 DSGVO nicht entfallen.[838] Der EDPB weist zudem darauf hin, dass das Fehlen einer Vereinbarung nicht mit dem faktischen Einfluss eines der gemeinsam Verantwortlichen gerechtfertigt werden könne.[839]

3. Rechtsprechung des EuGH

Welche Pflichten bei gemeinsam Verantwortlichen individuell wahrgenommen werden müssen und welche aufgeteilt werden können, ist bislang in der Rechtsprechung des EuGH kaum zu erkennen. So verlangte der EuGH im Urteil zu der Rechtssache Fashion ID[840] ein berechtigtes Interesse gem. Art. 7 lit. f DSRL[841] eines jeden gemeinsam Verantwortlichen als Verarbeitungsrechtfertigung.[842] Ebenso ordnete der EuGH den Verantwortlichen scheinbar jeweils individuell die Pflicht zur Einholung einer Einwilligung sowie die Erfüllung der korrespondierenden Informationspflichten zu.[843] Nach dem EuGH finden die individuellen Pflichten eines gemeinsam Verantwortlichen ihre Grenze darin, wie weit die jeweils eigene Verantwortlichkeit im Rahmen einer gemeinsamen Verantwortlichkeit reicht.[844] Ist ein individueller gemeinsam Verantwortlicher also für bestimmte Vorgänge nicht mehr verantwortlich, treffen ihn insoweit auch keine Pflichten. Dies ergibt sich aus dem vorgangsorientierten Ansatz des EuGH.[845] In Rn. 102 des Urteils zu der Rechtssache Fashion ID wird allerdings dem Websitebetreiber als gemeinsam Verantwortlichem die exklusive Verantwortung für die Einholung der Einwilligung explizit zugeordnet.[846] Eine wirksame Einwilligung

[836] *Schreiber*, ZD 2019, 55, 55.
[837] *Schreiber*, ZD 2019, 55, 56.
[838] Dies gilt a. für die Einwilligung, da die Informationspflichten aus Art. 12 ff. DSGVO nicht Art. 26 Abs. 1 S. 2, Abs. 2 DSGVO beinhalten.
[839] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 163.
[840] Dazu: Kapitel 4 B. III. Fashion ID.
[841] Mittlerweile Art. 6 Abs. 1 lit. f DSGVO.
[842] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 96.
[843] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 100.
[844] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 101.
[845] Dazu: Kapitel 4 L. II. Reichweite und Anteil der individuellen Verantwortlichkeit. EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70–74, 76.
[846] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102.

setze voraus, dass vor ihrer Erteilung die Informationspflichten gem. Art. 10 DSRL[847] gegenüber der betroffenen Person erfüllt würden.[848] In der Rechtssache Fashion ID könne der Plattformbetreiber die Einwilligung aber nicht vor Beginn der Verarbeitung einholen. Deswegen solle diese Pflicht durch den Websitebetreiber erfüllt werden. Auch die korrespondierenden Informationspflichten als Bedingung für eine wirksame Einwilligung solle exklusiv der Websitebetreiber erfüllen.[849] Wie mit dem Fall umzugehen wäre, dass erst für eine nachgelagerte Verarbeitung eine Einwilligung erforderlich wäre, spricht der EuGH, mangels entsprechender Vorlagefrage, nicht an.[850] Denkbar scheint es, in diesem Fall den Websitebetreiber auf vertraglicher Basis als „Boten"[851] des Plattformbetreibers zu nutzen.[852]

Was kann man aus den Ausführungen des EuGH nun ableiten? Zunächst muss für jeden gemeinsam Verantwortlichen individuell eine Verarbeitungsrechtfertigung gem. Art. 6 Abs. 1 DSGVO vorliegen.[853] Die Notwendigkeit einer individuellen Verarbeitungsrechtfertigung ergibt sich dabei auch aus der Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO. Denn diese trifft jeden (gemeinsam) Verantwortlichen individuell. Da die Verarbeitungsrechtfertigungstatbestände größtenteils auf den konkreten Verantwortlichen abstellen,[854] können deren Voraussetzungen offensichtlich zwischen gemeinsam Verantwortlichen divergieren.[855] So wäre es etwa bei der Verarbeitung aufgrund vertraglicher Beziehungen gem. Art. 6 Abs. 1 lit. b DSGVO notwendig, dass die gemeinsam Verantwortlichen jeweils Vertragspartei sind.[856] Bei den Verarbeitungsrechtfertigungstatbeständen nimmt die Einwilligung eine Sonderrolle ein, da diese eine

[847] Mittlerweile Art. 13 Abs. 1 DSGVO.

[848] A. abseits einer Einwilligung seien die Informationspflichten grundsätzlich vor der Erhebung zu erbringen: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 104 mit Verweis auf EuGH, Urteil vom 07.05.2009 – C-553/07 (Rijkeboer) = EuZW 2009, 546, Rn. 68; EuGH, Urteil vom 07.11.2013 – C-473/12 (IPI) = K&R 2014, 105, Rn. 23.

[849] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 103 ff.

[850] *Moos/Rothkegel*, MMR 2019, 584, 587.

[851] Dabei wäre noch zu klären, wie dies unionsrechtlich einheitlich zu bewerten wäre.

[852] Dies setzt aber voraus, dass der Plattformbetreiber bereit ist, die hierfür nötigen Informationen an den Websitebetreiber zu geben, vgl. die Parallelproblematik unter der Annahme der Websitebetreiber müsste a. hinsichtlich der Verarbeitungen durch den Plattformbetreiber informieren: EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 41.

[853] So a.: *Moos/Rothkegel*, MMR 2019, 584, 586. Anders scheinbar: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 166.

[854] Hinsichtlich eines Vertrags (lit. b), rechtlicher Verpflichtungen (lit. c), einer im öffentlichen Interesse liegenden Aufgabe (lit. e) oder des bereits genannten berechtigten Interesses (lit. f). Ausnahmen bilden hier nur die Einwilligung (lit. a) und das Schützen eines lebenswichtigen Interesses des Betroffenen (lit. d), die die betroffene Person als Bezugsobjekt haben.

[855] Vgl. BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 43.

[856] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 43.

aktive Handlung der betroffenen Person voraussetzt. Gerade bei nachgelagerten Verarbeitungsvorgängen wie in der Rechtssache Fashion ID ist eine rechtzeitige Einholung der Einwilligung häufig nur durch den Verantwortlichen, der direkten Kontakt mit der betroffenen Person hat, möglich.[857] Missverständlich ist daher eine Interpretation des Urteils, die annimmt, dass immer der (gemeinsam) Verantwortliche die Einwilligung einholen müsse, der die Verarbeitung initiiere. Diese Annahme gilt vielmehr nur dann, wenn den anderen gemeinsam Verantwortlichen keine Interaktion mit der betroffenen Person vor Beginn der Verarbeitung möglich ist.[858] Auch wenn eine solche Interaktion in der Praxis häufig nicht möglich sein wird, kann man gerade aufgrund der Ausführungen des EuGH[859] nicht von einer allgemeinen Gültigkeit dieser Annahme ausgehen.[860]

Abseits dieser zeitlich bzw. technisch bedingten Ausnahme bleibt unklar, ob der EuGH die Pflicht zur Einholung einer Einwilligung und zur Erfüllung der Informationspflichten den gemeinsam Verantwortlichen individuell zuweist. Die individuelle Erfüllung der Informationspflichten durch jeden gemeinsam Verantwortlichen stünde für die DSGVO jedenfalls im Widerspruch zu Art. 26 Abs. 1 S. 2 DSGVO. Sofern der Inhalt der Einwilligung hinsichtlich von Zwecken, Mitteln und relevanten Verarbeitungsvorgängen zwischen allen gemeinsam Verantwortlichen identisch ist, ist nicht ersichtlich, wieso die Pflicht zur Erfüllung der Informationspflichten nicht delegiert werden können sollte. Divergieren der Inhalt der Informationspflichten und der Einwilligung, ergibt eine individuelle Pflicht der gemeinsam Verantwortlichen wiederum Sinn, insbesondere im Hinblick auf den Grundsatz der Transparenz in Art. 5 Abs. 1 lit. a DSGVO. Somit ist bei nur partieller gemeinsamer Verantwortlichkeit aufgrund des vorgangsorientierten Ansatzes[861] grundsätzlich eine Einholung der Einwilligung samt damit verbundener Informationspflichten durch jeden gemeinsam Verantwortlichen

[857] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102. Siehe a.: *Monreal*, CR 2019, 797, Rn. 52. Inwiefern allerdings eine rechtzeitige Einholung der Einwilligung samt vorheriger Erfüllung der Informationspflichten in der Rechtssache Fashion ID durch den Websitebetreiber möglich sein soll, wenn die Erhebung der Daten bereits durch den Aufruf der Website stattfindet, bleibt zweifelhaft. Letztlich scheint nur eine Zwei-Klick-Lösung, also eine explizite Aktivierung des Plugins und folgende Nutzung, denkbar.

[858] So a.: *Kremer*, CR 2019, 676, Rn. 20; *Moos/Rothkegel*, MMR 2019, 584, 587; *Hanloser*, ZD 2019, 455, 460.

[859] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102.

[860] Wohl a.: *Kollmar*, NVwZ 2019, 1740, 1742.

[861] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70-74, 76.

notwendig,[862] jedenfalls sofern dies technisch und rechtzeitig möglich ist.[863] Eine anteilige Informationspflicht des einen gemeinsam Verantwortlichen mit ergänzenden Informationspflichten des anderen weiterverarbeitenden gemeinsam Verantwortlichen, soweit für dessen Verarbeitungsvorgänge keine gemeinsame Verantwortlichkeit mehr vorliegt, wäre kaum mit dem Grundsatz der Transparenz vereinbar.[864] Insofern ist die Aufteilung der Informationspflichten gem. Art. 26 Abs. 1 S. 2 DSGVO im Zusammenhang mit dem vorgangsorientierten Ansatz teleologisch zu reduzieren. Der EDPB äußert sich hierzu nur insoweit, dass ein gemeinsam Verantwortlicher die Pflicht habe, zu kontrollieren, ob ein anderer gemeinsam Verantwortlicher die personenbezogenen Daten für Zwecke jenseits derer, für die die Daten erhoben wurden, verarbeite.[865]

4. Position der Aufsichtsbehörden

Das WP 169 der Art. 29-Datenschutzgruppe enthielt ein Beispiel, das sich mit der Verteilung von Pflichten unter mehreren Akteuren beschäftigt. In Beispiel 13[866] (Banken und Informationspools über säumige Kunden) geht es um einen Informationspool mehrerer Banken, der zahlungssäumige Kunden zum Gegenstand hat.[867] Der Informationspool ist so konzipiert, dass alle Banken Informationen zu diesem beitragen und auf ihn Zugriff haben. Für die verantwortungstechnische Ausgestaltung eines solchen Informationspools sieht die Art. 29-Datenschutzgruppe grundsätzlich zwei Möglichkeiten: Zum einen gebe es die Variante, dass ein einzelner Betreiber bzw. „Zugangspunkt“[868] gegenüber betroffenen Personen den für Zugangs- und Löschungsanfragen individuell Verantwortlichen herausfinde und die Anfrage weitergebe. Die andere Variante sei der Betrieb des Informationspool durch eine eigene juristische Person, die als Verantwortlicher fungiere. In dieser Variante sollen die Banken als Schnittstelle zu dieser juristischen Person für Anfragen der betroffenen Personen dienen. Was genau aus dieser Rolle als Schnittstelle folgt, wird allerdings nicht weiter ausgeführt. In beiden

[862] So a.: *Golland*, K&R 2019, 533, 535; *Kremer*, CR 2019, 676, Rn. 19.

[863] Gerade im Hinblick auf die nachgeschaltete, nicht mehr gemeinsam verantwortete Verarbeitung durch den Plattformbetreiber in der Rechtssache Fashion ID stellt sich dort die Frage, wie dieser überhaupt informieren soll, sofern er nicht den Websitebetreiber als Boten nutzt.

[864] Kritisch: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 54. Folge wäre, dass sich die betroffene Person dann nämlich das Ausmaß der ursprünglich eingewilligten Verarbeitung und der weiteren Verarbeitung durch den weiterverarbeitenden Verantwortlichen selbst erschließen müsste.

[865] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 167.

[866] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 28.

[867] Vgl. *Kremer*, CR 2019, 225, Rn. 61.

[868] Dies leitet sich wohl vom englischen „point of contact“ ab.

Varianten wird nicht deutlich, ob nur eine Pflicht zur Weitergabe der Anfragen oder aber eine gemeinsame Verantwortlichkeit bestehe. Unklar ist auch, woraus sich eine solche Pflicht zur Weiterleitung ergeben solle.

5. Fazit

Die Delegation von Pflichten aus der DSGVO zwischen gemeinsam Verantwortlichen ist grundsätzlich möglich, gilt aber nicht für alle Pflichten. Betroffenenrechte können trotzdem gegenüber jedem gemeinsam Verantwortlichen geltend gemacht werden, auch wenn deren Erfüllung nur durch bestimmte gemeinsam Verantwortliche erfolgen kann.

VI. Störerauswahl bei aufsichtsbehördlichen Maßnahmen

Auf aufsichtsbehördlicher Ebene stellt sich bei mehreren Akteuren die Frage, nach welchen Kriterien eine Störerauswahl zu erfolgen hat.[869] Dabei ist der Störer derjenige Adressat, an den sich eine Maßnahme der Aufsichtsbehörde richtet. Eine Störerauswahl, wie sie sich aus dem Zusammenspiel von Art. 58 Abs. 4 DSGVO in Verbindung mit dem deutschen Verfahrensrecht ergibt,[870] muss zunächst den jeweiligen Tatbestand der maßgeblichen Norm beachten. So sehen die Untersuchungs- und Abhilfebefugnisse in Art. 58 Abs. 1 und 2 DSGVO üblicherweise entweder direkt, durch explizite Nennung, oder indirekt, per Normverweis, einen Adressaten vor. Regelmäßig ist dies der Verantwortliche. Ergibt sich ein Adressat weder aus der Norm selbst noch per Normverweis, ist es daher naheliegend – wenn auch nicht zwingend[871] – den Verantwortlichen als Adressaten in den Blick zu nehmen.[872]

Sofern die jeweilige Norm direkt oder indirekt einen oder mehrere Adressaten nennt, ist ein Vorgehen gegen jeden dieser Adressaten grundsätzlich rechtmäßig. Dies gilt, unabhängig vom Verhältnis der Verantwortlichkeit, auch bei gemeinsam Verantwortlichen.[873] Denn eine bestimmte Rangordnung verschiedener Adressaten kennt das

[869] Vgl. hierzu a. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 343 ff.

[870] Hierzu: *Schreiber*, ZD 2019, 55, 58 f.; Paal/Pauly/*Körffer*, Art. 58 DSGVO, Rn. 31; für die DSRL: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 29. Allgemein zur Störerauswahl im Polizei- und Ordnungsrecht: *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 171 ff.

[871] Dazu: Kapitel 5 K. Rückgriff auf Adressaten des allgemeinen Polizei- und Ordnungsrecht.

[872] So a.: *Schreiber*, ZD 2019, 55, 60.

[873] Dazu: Kapitel 4 L. II. 2. Anteil oder Verhältnis der Verantwortlichkeit; *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 145. Vgl. a. ErwGr 79; S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 2.

Verwaltungsrecht nicht.[874] Demnach können alle oder nur einzelne Adressaten herangezogen werden.[875] Häufig wird es sich bei gemeinsam Verantwortlichen ohnehin anbieten, alle gemeinsam Verantwortlichen mit derselben Abhilfemaßnahme zu belegen,[876] insbesondere, um der fehlenden Erfüllungsfähigkeit eines gemeinsam Verantwortlichen zu begegnen. Maßgeblich für die Ausübung des Ermessens im Rahmen der Störerauswahl ist der Grundsatz der Effektivität der Gefahrenabwehr.[877] Im Kern muss also anhand der Störerauswahl eine möglichst wirksame und schnelle Beseitigung der Gefahr erfolgen. Daneben soll die Störerauswahl zwar auch Aspekte der Verhältnismäßigkeit berücksichtigen,[878] etwa Leistungs- bzw. Erfüllungsfähigkeit des Störers, Zumutbarkeit, Sachnähe, Schadensnähe sowie Verursachungs- und Verschuldensbeitrag.[879] Dies gilt allerdings nur so weit, wie dadurch nicht die Effektivität der Gefahrenabwehr beeinträchtigt wird. Überlange Untersuchungen zum Verursachungsbeitrag etwa sind demnach also nicht angebracht. Andererseits sind Abhilfemaßnahmen gegenüber individuellen gemeinsam Verantwortlichen, die einer Verpflichtung weder selbst noch mittels Einwirkung auf die anderen gemeinsam Verantwortlichen nachkommen können, denen also die Befolgung einer Abhilfemaßnahme autonom schlicht nicht möglich ist, auch nicht angebracht.[880] Dies ergibt sich bereits aus dem Begriff der Effektivität. Bei gleicher Effektivität wäre zudem der Eingriff mit der geringsten Beeinträchtigung für den jeweiligen Adressaten zu wählen.[881]

Sollte das Verhältnis der Verantwortlichkeit[882] bekannt und plausibel sein, spricht nichts dagegen, den gemeinsam Verantwortlichen mit dem überwiegenden Verhältnis der Verantwortlichkeit als primären Adressaten zu belangen.[883] Sinnvoller erscheint

---

[874] *Schreiber*, ZD 2019, 55, 59 m.w.N.

[875] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 60.

[876] Dies gilt offensichtlich für die Untersuchungsbefugnisse, so a.: *Schreiber*, ZD 2019, 55, 60.

[877] BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 30; BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 61; *Bäcker*, D. Polizeiaufgaben und Regelungsmuster des polizeilichen Eingriffsrechts, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 208 ff. Vgl. für das Baurecht OVG Lüneburg, Beschluss vom 19.12.2018 – 1 ME 155/18 = NVwZ 2019, 334.

[878] Siehe etwa § 2 Abs. 1 PolG RLP. Zum alten BDSG a.F.: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 18, 29. Vgl. für das Baurecht: OVG Lüneburg, Beschluss vom 19.12.2018 – 1 ME 155/18 = NVwZ 2019, 334, 336.

[879] Vgl. *Schreiber*, ZD 2019, 55, 59.

[880] Letzteres ergibt sich schon aus der fehlenden Geeignetheit der Maßnahme im Rahmen der Verhältnismäßigkeit.

[881] So a. § 2 Abs. 1 PolG RLP.

[882] Dazu: Kapitel 4 L. II. 2. Anteil oder Verhältnis der Verantwortlichkeit.

[883] Die Aufsichtsbehörde soll nach Ansicht des EDPB allerdings nicht an die Vereinbarung gem. Art. 26 Abs. 1 S. 2 DSGVO gebunden sein: *European Data Protection Board*, Guidelines 07/2020 on the con-

demgegenüber allerdings die Überlegung, wer im konkreten Fall tatsächlich am schnellsten der maßgeblichen Pflicht und der aufsichtsbehördlichen Abhilfemaßnahme nachkommen kann. Dabei kann eine Vielzahl von Faktoren relevant sein. Nahe liegt es etwa, die Abhilfemaßnahmen an denjenigen Verantwortlichen zu richten, der die technischen Möglichkeiten hat, der Pflicht nachzukommen bzw. die Gefahr zu beseitigen.[884] Gemeinsam Verantwortliche können durchaus unterschiedliche technische Einflussmöglichkeiten haben, die sich auch in ihrer Intensität unterscheiden können. Dabei sollte die Frage, ob jemand Besitz an der verarbeitenden Hardware, etwa einem Server, hat oder nur entsprechende Zugriffsrechte besitzt, irrelevant sein.[885] Im Urteil des EuGH in der Rechtssache Wirtschaftsakademie[886] etwa hätte der Plattformbetreiber die fehlenden Informationen gem. Art. 13 DSGVO zwar recht einfach bereitstellen und das Webseitenlayout entsprechend anpassen können. Allerdings bestand für den Betreiber der Fanpage immer noch die, zugegebenermaßen drastische, Möglichkeit, die Seite zu deaktivieren.[887] Kommen in solch einem Sachverhalt noch andere Faktoren hinzu, wie etwa die schwierige Durchsetzbarkeit der aufsichtsbehördlichen Maßnahme im EU-Ausland, die fragwürdige Entscheidungsautonomie der EU-Niederlassung eines nicht-EU-Unternehmens sowie deren zweifelhafte Erreichbarkeit, kann es durchaus angebracht sein, auch den Adressaten mit der drastischeren Einwirkungsmöglichkeit als Adressaten auszuwählen.[888] Daneben kann es in der Gesamtschau verschiedener Faktoren aber auch durchaus sinnvoll sein, denjenigen Verantwortlichen als Adressaten auszuwählen, der nur rechtliche Einflussmöglichkeiten, etwa durch Vertrag oder aufgrund gesellschaftsrechtlicher Stellung, hat.[889] Letztlich bietet es sich an, allein aus Gründen der reibungslosen Durchführung der Abhilfemaßnahmen, alle potenziellen Adressaten in eine Maßnahme einzubeziehen. Dabei kann, wenn die Aufsichtsbehörde

cepts of controller and processor in the GDPR, 07.07.2021, Rn. 191. Nach Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 24 soll die Vereinbarung den Aufsichtsbehörden ermöglichen Kontroll- und Überwachungsmaßnahmen durchzuführen.

[884] *Schreiber*, ZD 2019, 55, 60.

[885] Anders: *Schreiber*, ZD 2019, 55, 60.

[886] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[887] Dies war a. ermessensfehlerfrei im Hinblick auf die Erforderlichkeit der Maßnahme: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 32.

[888] Vgl. BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 31; vgl. zu der Rechtssache Google Spain *Masing*, https://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/ (abgerufen am 17.07.2024).

[889] Anders: *Schreiber*, ZD 2019, 55, 60.

einen potenziellen Adressaten ignoriert,[890] allerdings auch ein Ermessensausfall vorliegen. Insgesamt bleibt die Störerauswahl stark abhängig von den Details des Einzelfalls.[891]

M. Schlussfolgerungen aus der Analyse - Die Unterkomplexität des Verantwortlichkeitskonzeptes

I. Neuerungen der DSGVO?

Insofern der Unionsgesetzgeber durch Art. 26 DSGVO eine klare Zuteilung von Verantwortung innerhalb des Datenschutzrechts erreichen und damit auch der Komplexität von vernetzten Verarbeitungsstrukturen[892] begegnen wollte,[893] scheint dies deutlich misslungen.[894] Denn zum einen gab es das Konzept der gemeinsam Verantwortlichen bereits knapp 20 Jahre vor der DSGVO schon in Art. 2 lit. d DSRL.[895] Zum anderen regelt Art. 26 DSGVO, als die inhaltliche Neuerung gegenüber der DSRL, überwiegend gerade nicht die Voraussetzungen, sondern nur die Folgen der gemeinsamen Verantwortlichkeit.[896] Folge der gemeinsamen Verantwortlichkeit ist im Rahmen der Vereinbarung dabei vor allem die Offenlegung der individuell übernommen Pflichten (Art. 26 Abs. 1 S. 2 DSGVO) und fakultativ die Angabe einer Anlaufstelle für die betroffenen Personen (Art. 26 Abs. 1 S. 3 DSGVO).

Damit ein gemeinsam Verantwortlicher aber die sich aus seiner Qualifizierung als solcher ergebenden Folgen beachten kann, muss er notwendigerweise zuerst einmal

---

[890] *Schreiber*, ZD 2019, 55, 59.

[891] Einlenkend: *Schreiber*, ZD 2019, 55, 60.

[892] Vgl. den Begriff der mehrstufigen Anbieterverhältnisse BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 439.

[893] BeckOK DatenschutzR[47]/*Spoerr*, Art. 26 DSGVO, Rn. 6; Ehmann/Selmayr/*Bertermann*, Art. 26 DS-GVO, Rn. 1; *Wagner*, ZD 2018, 307, 308; *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, 61.

[894] Ähnlich: *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 68; vgl. a. die Kritik von *Alsenoy*, CLSR[28] (2012), 25, 40 f. zu *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010. Vgl. Kritik allgemein hinsichtlich der Konzepte des Verantwortlichen und Auftragsverarbeiters *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 2 Fn. 10 m.w.N. Ironisch wirkt dabei, dass die Kommission in den Jahren 2003 und 2007 keinen Reformbedarf festgestellt hatte: COM (2003) 265; COM (2007) 87.

[895] Dazu: Kapitel 1 B. V. DSRL (1995). *Specht-Riemenschneider/Schneider*, MMR 2019, 503, 504.

[896] *Schreiber*, ZD 2019, 55, 55.

feststellen, dass er überhaupt gemeinsam Verantwortlicher ist.[897] Art. 26 Abs. 1 S. 1 DSGVO wiederholt hinsichtlich der Voraussetzungen einer gemeinsamen Verantwortlichkeit aber im Wesentlichen nur die Definition aus Art. 4 Nr. 7 DSGVO.[898] Statt der gemeinsamen Entscheidung über die Zwecke und Mittel der Verarbeitung spricht Art. 26 DSGVO von der gemeinsamen Festlegung der Zwecke und Mittel. Aufgrund des leicht abweichenden Wortlauts gegenüber Art. 4 Nr. 7 DSGVO wird durch diese erneute Definition statt einer Klärung der Voraussetzungen eher noch Verwirrung gestiftet.[899] Einen gewissen Mehrwert bietet die Definition aus Art. 26 Abs. 1 S. 1 DSGVO allerdings zugegebenermaßen dahingehend, dass zwei oder mehr Verantwortliche gemeinsam Verantwortliche sein können. Aber auch hier stellt sich bei genauer Analyse des Wortlauts die Frage, ob die gemeinsam Verantwortlichen unabhängig von der gemeinsamen Verantwortlichkeit bereits verantwortlich sein müssen und falls ja, wofür überhaupt.

Die entscheidende Voraussetzung „gemeinsam" wird ebenso wie „festlegen" nicht weiter erläutert. Ist die Verantwortlichkeit nach dem Urteil des EuGH in der Rechtssache Fashion ID anhand des individuellen Verarbeitungsvorgangs zu beurteilen,[900] so ist das Verständnis der Definitionselemente „gemeinsam" und „festlegen" aber maßgeblich für die Qualifizierung eines Akteurs als gemeinsam Verantwortlicher. Somit sind allein auf Grundlage der DSGVO die Voraussetzungen eines gemeinsam Verantwortlichen derart unbestimmt, dass man dies adäquat mit den folgenden Worten des verstorbenen Associate Justice of the Supreme Court Potter Stewart beschreiben kann:

> *„I know it when I see it."*[901]

[897] *Mahieu/van Hoboken/Asghari*, JIPITEC 2019, 85, Rn. 65; G/S/S/V/*Veil*, Art. 26 DSGVO, Rn. 73; *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 168 ff.; zu potenziellen Anwendungsfällen: Taeger/Gabel/*Lang*, Art. 26 DSGVO, Rn. 2.

[898] Dazu: Kapitel 4 C. I. Art. 4 Nr. 7 vs. Art. 26 Abs. 1 S. 1 DSGVO – unterschiedliche Definitionen der gemeinsam Verantwortlichen? Was der Mehrwert einer Wiederholung gegenüber einer Aufnahme als individuelle Definition in Art. 4 DSGVO ist, weiß vermutlich nur der Rat. Allerdings gab es auch im Rat unzufriedene Stimmen hinsichtlich der Voraussetzungen der gemeinsam Verantwortlichen, vgl. Ratsdokument 9398/15, S. 149, Fn. 383.

[899] Vgl. *Monreal*, CR 2019, 797, Rn. 8 ff.

[900] Dazu:Kapitel 4.L. II. Reichweite und Anteil der individuellen Verantwortlichkeit.

[901] Der ursprüngliche Kontext war die Frage, ob es sich in dem, dem Supreme Court vorgelegten, Sachverhalt (*Jacobellis v. Ohio*, 378 U.S. 184 (1964)) um Hard-Core-Pornographie handelte.

II. Fokus auf die betroffene Person

Art. 26 DSGVO stellt zweifelsfrei gegenüber der betroffenen Person einen Mehrwert an Transparenz her, insbesondere durch die Richtigkeits- und Zugänglichkeitsanforderung des Art. 26 Abs. 2 DSGVO. Ob diese Anforderungen im Hinblick auf die Verpflichtung aller gemeinsam Verantwortlichen als Ansprechpartner nach Art. 26 Abs. 3 DSGVO überhaupt erforderlich sind, ist allerdings fraglich. Insgesamt schafft Art. 26 DSGVO nur gegenüber der betroffenen Person eine klare Zuteilung der jeweiligen Verantwortung.[902] Durch die fehlende Präzisierung der Voraussetzungen einer gemeinsamen Verantwortlichkeit besteht gerade für datenschutzrechtliche Akteure keine Rechtssicherheit, wann sie das Risiko einer gemeinsamen Verantwortlichkeit trifft. Auch die Aufteilung der Pflichten zwischen gemeinsam Verantwortlichen wird in Art. 26 DSGVO nur insoweit geregelt, dass die gemeinsam Verantwortlichen dies selbst unter sich klären müssen. Als Kehrseite dieser rudimentären Regelung der gemeinsamen Verantwortlichkeit müssen Aufsichtsbehörden langwierige Untersuchungen oder unberechenbare Gerichtsverfahren gegenüber potenziellen gemeinsam Verantwortlichen eingehen, sofern ihre Ressourcen dies überhaupt zulassen.

Die Unterkomplexität der Voraussetzungen der gemeinsam Verantwortlichen wirkt dabei umso verwunderlicher, wenn man die Detailliebe der Vorgaben für die Auftragsverarbeitung in Art. 28 DSGVO betrachtet. Die hochkomplexe Realität von dezentral vernetzten und verschachtelten Verarbeitungen wird durch die alleinige Regelung der Folgen der gemeinsamen Verantwortlichkeit in Art. 26 DSGVO hingegen nicht annähernd adäquat erfasst. Es gelten vielmehr die gleichen Voraussetzungen für die gemeinsame Verantwortlichkeit wie bereits unter der DSRL. Wie anhand der Urteile des EuGH den Rechtssachen in Wirtschaftsakademie und Fashion ID[903] deutlich wird, gilt dabei nach wie vor ein „alles oder nichts"-Prinzip. Entweder man ist (gemeinsam) Verantwortlicher oder eben nicht. Die Auftragsverarbeitung kann mit ihrer spezifischen Voraussetzung der Weisungsgebundenheit kaum Defizite der Verantwortlichkeitsrollen flexibel kompensieren. Das Rollen- oder Verantwortlichkeitsmodell der

[902] Damit entspricht Art. 26 DSGVO weitgehend der Stellungnahme des EDPS vom 12.07.2012: *Hustinx*, https://www.edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf (abgerufen am 17.07.2024) Rn. 183.

[903] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

DSGVO kennt schlicht keine Verantwortungsrolle abseits des Verantwortlichen, gemeinsam Verantwortlichen oder Auftragsverarbeiters.[904] Diese Rollen können aber, abseits des Auftragsverarbeiters mit seiner besonderen Voraussetzung der Weisungsgebundenheit, nicht hinsichtlich des Beteiligungsgrades an einer Verarbeitung und damit einhergehend einer Verantwortung hierfür differenzieren. Die datenschutzrechtlichen Verantwortungsrollen können also in Verarbeitungsszenarien mit mehreren Akteuren nicht flexibel Verantwortung zuweisen. So notwendig die Einheitlichkeit der Verantwortungsrolle aus Sicht der Betroffenenrechte erscheint, so unterkomplex wirkt sie aus Sicht der verarbeitenden Akteure und der Aufsichtsbehörden. Ziel sollte sein, die einheitliche Wahrnehmung der Betroffenenrechte zu garantieren und gleichermaßen eine differenzierte Berechenbarkeit der Verantwortung für verarbeitende Akteure und Aufsichtsbehörden herzustellen. Rechtssicherheit bezüglich der Verantwortung und Haftung der Verantwortlichen,[905] wie sie ErwGr 79 DSGVO vorsieht, wird mit dem momentanen Verantwortlichkeitsmodell also gerade nicht erzielt. Allenfalls im Innenverhältnis profitieren die gemeinsam Verantwortlichen durch die Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO von einer Fixierung der jeweiligen Verantwortung und somit einer vertraglichen Haftung.[906]

III. Breite Anwendung des Konzeptes der gemeinsamen Verantwortlichkeit durch den EuGH

In der Rechtsprechung des EuGH lässt sich immer wieder die Tendenz erkennen, die erkennbare Unterkomplexität der Verantwortungsrollen[907] mit Hilfe der gemeinsamen Verantwortlichkeit zu kompensieren. So ist anhand der Urteile in den Rechtssachen Wirtschaftsakademie, Jehovan todistajat, Fashion ID, NZÖG und IAB Europe[908] deutlich zu erkennen, dass der EuGH das Konzept der gemeinsamen Verantwortlichkeit weit auslegt. Allerdings dürfte es langfristig zu Sachverhalten kommen, in denen auch bei großzügiger Auslegung der Voraussetzung der „gemeinsamen Entscheidung" Akteure nicht mehr als gemeinsam Verantwortliche erfasst werden können. Dieses Defizit

[904] Vgl. a. die Kritik bei *Golland*, ZD 2020, 397, 402.

[905] Vgl. a. *Blazy*, § 5 Pflichten des Verantwortlichen I. Verantwortung für die Datenverarbeitung, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, 2018, Rn. 12.

[906] Vgl. Paal/Pauly/*Martini*, Art. 26 DSGVO, Rn. 10.

[907] Vgl. zur Intransparenz *Roßnagel*, MMR 2005, 71, 72.

[908] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

müsste dann, wie der EuGH bereits angedeutet hat, möglicherweise über das mitgliedstaatliche Recht abgedeckt werden.[909] Denkbar wäre es darüber hinaus, wie es das BVerwG in der Wirtschaftsakademie-Vorlage erwogen hat, die sorgfältige Auswahl des Auftragsverarbeiters, jedenfalls im kommerziellen Bereich, auf solche Sachverhalte entsprechend auszudehnen.[910]

IV. Fazit

Mangels weiterer Verantwortungsrollen dürften immer mehr Grenzfälle[911] unter das Konzept der gemeinsam Verantwortlichen subsumiert werden.[912] Eine solche Rechtsprechung wird aber auch dazu führen, dass die Grenzen des Verantwortlichen insgesamt erodieren, da einzelne Definitionselemente ohne systematisches Fundament zunehmend an Bedeutung verlieren.[913] Andererseits leidet unter der weiten Auslegung der gemeinsamen Verantwortlichkeit auch das Konzept des Auftragsverarbeiters. Denn auch der Auftragsverarbeiter hat durchaus gewisse Spielräume innerhalb des Weisungsrechts des Verantwortlichen. Die Problematik von Grenzfällen der Verantwortlichkeit wird durch die weite Anwendung der gemeinsamen Verantwortlichkeit insgesamt nicht gelöst. Sie wird nur in die Definitionselemente des Verantwortlichen verschoben. Gleichzeitig leidet die Rechtssicherheit für die Verantwortlichen.[914]

Wünschenswert wäre es daher, die bislang erkennbaren Grenzfälle der Verantwortlichkeit, die nicht in die klassischen Verantwortungsrollen passen, über neue, enger umrissene Verantwortungsrollen zu erfassen. Dies würde die Definitionselemente des Verantwortlichen kohärent halten und gleichzeitig verdeutlichen, dass diese noch zu schaffenden Verantwortungsrollen Ausnahmecharakter besitzen. Denkbar wäre es beispielsweise, die Ermöglichung von Verarbeitungen, etwa durch Auswahl eines Anbieters oder Nutzung einer Infrastruktur, gesondert zu regeln.[915] Dafür müsste entweder der EuGH rechtsfortbildend oder aber der Unionsgesetzgeber selbst tätig werden. Grund-

[909] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74.

[910] BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 438 siehe Vorlagefrage 2.

[911] Zu möglichen Anwendungsfällen: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 95 f.

[912] Vgl. die weichen Kriterien bei *Bock*, K&R 2019, 30, 33, die kaum über die Definition hinausgehen.

[913] Kritisch a.: S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 53 ff.

[914] *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 260 spricht von einer „[...] breitflächige[n] Dysfunktionalität des Gesamtkonzepts durch organisierte Verantwortungslosigkeit [...]".

[915] Vgl. die Kritik bei *Schleipfer*, CR 2019, 579, 580 f.

legende Reformen am Konzept des Verantwortlichen in nächster Zeit sind jedoch extrem unwahrscheinlich. Trotzdem spricht nichts dagegen, wenigstens grundlegende Typisierungen von Verantwortungsrollen zu bilden, die langfristig gesetzlich aufgenommen werden könnten.

Kapitel 5

Ansätze zur Überarbeitung des Konzeptes der Verantwortlichkeit

In diesem Abschnitt werden Ansätze für eine Überarbeitung. des Konzeptes der Verantwortlichkeit dargestellt und bewertet sowie ein Ausblick für die weitere Entwicklung der Verantwortlichkeit gegeben. Die Defizite im Konzept der Verantwortlichkeit sind nicht neu.[1] Durch die rasante technische Entwicklung der letzten Jahrzehnte sind sie aber immer weiter sichtbar geworden. Die Diskussion um die Verantwortlichkeit, insbesondere die gemeinsame Verantwortlichkeit, ist trotzdem erst aufgrund der massiv erhöhten Sanktionsmöglichkeiten durch die DSGVO[2] sowie der jüngeren Rechtsprechung des EuGH[3] wieder intensiver geworden. Diese Diskussion war zuletzt davon geprägt, die Voraussetzungen der gemeinsamen Verantwortlichkeit anhand der Rechtsprechung des EuGH zu analysieren und Ansätze dafür zu finden deren vermeintlich weiten Anwendungsbereich zu beschränken. Dabei wird auf die Erfüllung kumulativer Voraussetzungen bestanden, es werden ungeschriebene Voraussetzungen wie die Erheblichkeitsschwelle eines Entscheidungsbeitrags vorgeschlagen oder Voraussetzungen werden schlicht sehr eng ausgelegt.[4] Ziel dieser Bemühungen scheint die Rückbesinnung auf die scheinbar bewährten Konzepte des singulären Verantwortlichen und des Auftragsverarbeiters zu sein. Das Konzept der gemeinsamen Verantwortlichkeit soll also eine Ausnahmeerscheinung darstellen. Abseits dessen finden sich kaum Vorschläge zu einer Überarbeitung oder Ausdifferenzierung des Konzeptes der Verantwortlichkeit. Auch der EDPB, als Nachfolgegremium der Art. 29-Datenschutzgruppe, reagiert bislang nur mit Analysen auf die Rechtsprechung des EuGH.[5] Er zeigt keine Ansätze für eine Ausdifferenzierung oder Überarbeitung des Verantwortlichkeitskonzeptes der DSGVO auf. Insgesamt ist bei der Diskussion um das Konzept der Verantwortlichkeit

[1] Dazu: Kapitel 1 B. IX. Kritik der fehlenden Evolution des Konzeptes.
[2] Insb. Art. 83 DSGVO.
[3] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.
[4] Dazu: Kapitel 4.
[5] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021, Rn. 46 ff.

bislang erkennbar, dass zwar sehr spezifische Elemente diskutiert werden, dabei allerdings häufig die Perspektive auf die systematischen Auswirkungen und die Durchsetzung unberücksichtigt bleibt. Diese Fixierung auf bestimmte Elemente der Verantwortlichkeit scheint selbst der EuGH zu verfolgen, wie der vorgangsorientierte Ansatz im Urteil zu Rechtsache Fashion ID zeigt.[6] Eine Systematik in der Rechtsprechung ist daher regelmäßig kaum zu erkennen.

Da immer wieder nur spezifische Elemente der gemeinsamen Verantwortlichkeit die Diskussion um die Verantwortlichkeit beherrschen, ist die Zahl neuer Ansätze für das Konzept der Verantwortlichkeit insgesamt überschaubar. Einige der älteren Ansätze sind in der erweiterten Normierung der gemeinsamen Verantwortlichkeit in der DSGVO aufgegangen,[7] andere Ansätze sind gesetzgeberisch insgesamt überholt. Viele der verbleibenden älteren Ansätze sind allerdings nach wie vor erwägenswert. Neben grundsätzlichen Änderungen am Konzept der Verantwortlichkeit können durch Ansätze über den Anwendungsbereich der DSGVO spezifische Defizite des Konzeptes der Verantwortlichkeit kompensiert werden. Bei den hier analysierten Ansätzen handelt es sich um Ansätze nach geltendem Recht (de lege lata), wie auch nach noch zu schaffendem Recht (de lege ferenda). Dies wird im jeweiligen Kapitel vermerkt. Soweit diese Ansätze einer Gesetzesänderung bedürfen, scheint es zudem sinnvoll, sie zeitlich zu befristen, um ihre Wirksamkeit zu evaluieren.[8]

Grundsätzlich lassen sich die Ansätze zur Überarbeitung des Konzeptes der Verantwortlichkeit in sieben Kategorien einteilen:

- Rückbesinnung auf die klassischen Rollen des singulären Verantwortlichen und Auftragsverarbeiters („Getrennte Verantwortlichkeiten“)
- Typologie häufiger Verantwortlichkeitsszenarien („Typologie der Verantwortlichkeit“)
- Ausdifferenzierung der konkreten Voraussetzungen der jeweiligen Rollen[9]
- Modifikation der bestehenden Rollen („Datenschutzrechtliche Gesamtschuldnerschaft“, „Anwendung der DSA-Privilegierungen“)

[6] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 70 ff.

[7] So wohl die nachhaltige Verantwortlichkeit: *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 18.03.2010, 15 f.

[8] Vgl. bereits 1987 *Simitis*, CR 1987, 602, 613; *Lennartz*, RdV 1990, 25, 28 f.

[9] Dazu:
Kapitel 2 und Kapitel 4.

- Erweiterung und Schematisierung der Rollen („Auswahlverantwortlichkeit", „Datenschutzrechtliche Beihilfe", „Herstellerverantwortlichkeit", „Intermediärsverantwortlichkeit")
- Modifikation des Anwendungsbereichs („Haushaltsausnahme")
- Auffangkonstruktionen („Störerhaftung und Zweckveranlasser", „Rückgriff auf Störerauswahl im allgemeinen Polizei- und Ordnungsrecht")

Die folgende Darstellung orientiert sich dabei daran, wie stark die DSGVO modifiziert werden müsste sowie nach dem Ansatzpunkt einer solchen Modifikation.

A. Getrennte Verantwortlichkeiten

Da sich die Feststellung einer gemeinsamen Verantwortlichkeit aufgrund der unklaren Rechtsprechung des EuGH bislang schwierig gestaltet, wird von Teilen der Literatur vorgeschlagen, statt einer gemeinsamen Verantwortlichkeit mehrerer Akteure einfach von getrennten Verantwortlichkeiten auszugehen.[10] Hierbei handelt es sich um einen Ansatz, der bereits nach geltendem Recht verfolgt werden könnte. Dieser Ansatz, von getrennten Verantwortlichkeiten auszugehen, basiert auf der Prämisse, dass die gemeinsame Verantwortlichkeit zwingend einen gemeinsamen Zweck voraussetze.[11] Grundsätzlich lässt sich hinsichtlich getrennter Verantwortlichkeiten erkennen, dass für die betroffenen Personen weder erkennbare Vor- noch Nachteile entstehen.[12] Hinsichtlich des Schadensersatzes setzt etwa Art. 82 Abs. 4 DSGVO nicht notwendigerweise eine gemeinsame Verantwortlichkeit der beteiligten Verantwortlichen für eine Gesamtschuld voraus. Auch die Informationspflichten gem. Art. 12 ff. DSGVO müssen entsprechend der Rechtsprechung aus der Rechtssache Fashion ID[13] ohnehin nur für mitverantwortete Vorgänge befolgt werden.

Bei aller berechtigter Kritik an den Ausführungen des EuGH zu dem Zweck[14] in den Urteilen in den Rechtssachen Wirtschaftsakademie und Fashion ID ist allerdings bereits die Annahme der zwingenden Voraussetzung eines gemeinsamen Zweckes

[10] So etwa: *Moos/Rothkegel*, MMR 2019, 584, 586; *Lee/Cross*, MMR 2019, 559, 562. Kritisch: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 79 ff.
[11] *Moos/Rothkegel*, MMR 2019, 584, 585; *Lee/Cross*, MMR 2019, 559, 561 f.
[12] *Lee/Cross*, MMR 2019, 559, 562.
[13] Dazu: Kapitel 4 B. III. Fashion ID.
[14] Gerade in Bezug auf den unklaren Begriff des Interesses oder der Zweckeinheit.

falsch.[15] Daneben stellen sich bei einer getrennten Verantwortlichkeit vielfach auch praktisch erhebliche Hürden. So hat der EuGH im Urteil zu der Rechtssache Fashion ID festgestellt, dass die Einholung der Einwilligung sowie die dazu notwendige Erbringung der Informationspflichten gegenüber der betroffenen Person nur durch den Websitebetreiber (einem gemeinsam Verantwortlichen) als erstem Kontaktpunkt erfolgen kann.[16] Die gemeinsame Verantwortlichkeit ermöglicht in bestimmten Verarbeitungsszenarien also aufgrund der Aufteilung der Pflichten nach Art. 26 Abs. 1 S. 2 DSGVO überhaupt erst eine rechtmäßige Datenverarbeitung. Ebenso übersieht der Vorschlag getrennter Verantwortlichkeiten, dass in Ermangelung einer gemeinsamen Verantwortlichkeit keine Delegation bestimmter Teilentscheidungen möglich wäre und der jeweils (singulär) Verantwortliche allein über die Zwecke der Verarbeitung wie auch alle Aspekte der Mittel der Verarbeitung entscheiden müsste.[17] Die alleinige Entscheidung über die Zwecke und alle Elemente der Mittel war in den Sachverhalten, die dem EuGH bislang vorlagen, aber gar nicht möglich.[18] So konnte der Fanpage- bzw. Websitebetreiber nur über seine eigenen Zwecke sowie bestimmte Elemente der Mittel mitentscheiden. Eine getrennte Verantwortlichkeit wäre in den entsprechenden Sachverhalten schon per definitionem nicht möglich gewesen. Der Plattformbetreiber wäre nach diesem Ansatz in beiden Fällen allein verantwortlich gewesen. Allerdings hätte die maßgebliche Verarbeitung ohne den Beitrag des Fanpage- bzw. Websitebetreibers gar nicht erst stattgefunden. Gleichzeitig ist aber, auch bei Ablehnung des Ansatzes getrennter Verantwortlichkeiten, einzuräumen, dass nicht alle Verarbeitungsszenarien, in denen irgendeine Art von Zusammenarbeit unterschiedlicher Akteure vorliegt, automatisch eine gemeinsame Verantwortlichkeit darstellen.[19]

B. Typologie der Verantwortlichkeit

Wie bereits erwähnt, ist das Verantwortlichkeitsmodell der DSGVO vergleichsweise simpel. Positiv erfasst werden nur der Verantwortliche als singulär oder gemeinsam Verantwortlicher und der Auftragsverarbeiter. Aufbauend auf dieses Modell könnten

[15] Dazu: Kapitel 4 E. II. Die „Einwilligung“ in eine Verarbeitung als Einigung auf einen gemeinsamen Zweck?

[16] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 102 f.

[17] Daher insgesamt fernliegend: *Lee/Cross*, MMR 2019, 559, 562.

[18] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[19] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 24. So unterstellend: *Moos/Rothkegel*, MMR 2019, 584, 586.

aber verschiedene Arten von Verantwortlichen und Auftragsverarbeitern typisiert werden.[20] Denkbar ist es, dabei häufig auftretende Varianten einer Verantwortlichkeit oder Auftragsverarbeitung zu erfassen, um einer detaillierten Prüfung der Verarbeitung zur Verantwortlichkeitsanalyse vorzubeugen. Sofern es hier nur um Leitlinien der Aufsichtsbehörden ginge, wäre dies ein Ansatz nach geltendem Recht. Ebenso wäre es aber auch denkbar, ausgehend vom Grundmodell des Verantwortlichen oder Auftragsverarbeiter, im Rahmen der Typisierung, weitere Pflichten oder Privilegierungen an bestimmte Arten von Verantwortlichen oder Auftragsverarbeitern zu knüpfen. Dies wäre ein Ansatz nach noch zu schaffendem Recht. Denkbar wäre eine solche Typisierung insbesondere im Hinblick auf Plattformen, dezentrale Strukturen sowie Telekommunikationsakteure. Auch die datenschutzrechtliche Verantwortlichkeit im Kontext der Nutzung von LLMs könnte einer näheren Typisierung unterzogen werden.

Als Orientierung für eine solche Typologie könnte etwa die Musterbauordnung[21] dienen. Die Musterbauordnung dient der föderalen Koordination der Landesbauordnungen. Dieses Muster legt in § 52 MBO die Grundverantwortlichkeit des Bauherrn und der anderen am Bau Beteiligten für die Einhaltung der öffentlich-rechtlichen Vorschriften fest.[22] Die Normvorschläge §§ 53 bis 56 MBO legen die jeweiligen Besonderheiten für den Bauherrn, den Entwurfsverfasser, die Unternehmer und die Bauleiter fest. So muss der Bauherr etwa nach § 53 Abs. 1 S. 1 MBO unter bestimmten Bedingungen geeignete Beteiligte nach Maßgabe der §§ 54 bis 56 MBO bestellen, soweit er nicht selbst zur Erfüllung der Verpflichtungen nach diesen Vorschriften geeignet ist. Der Entwurfsverfasser nach § 54 MBO ist wiederum nur für spezifische Punkte verantwortlich, etwa die Vollständigkeit und Brauchbarkeit seines Entwurfs gem. § 54 Abs. 1 S. 2 MBO.

Für die DSGVO könnte man den Verantwortlichen als Grundlage nehmen und davon ausgehend weitere an einer Verarbeitung Beteiligte regeln, etwa den Hersteller[23]

[20] Ähnlich mit der sehr abstrakten Unterscheidung primärer und sekundärer Verantwortlichkeit: *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 302 ff.

[21] Musterbauordnung - MBO - Fassung November 2002, zuletzt geändert durch Beschluss der Bauministerkonferenz vom 23./24.11.2023 (https://www.bauministerkonferenz.de/IndexSearch.aspx?method=get&File=bya892ba82y1b9bbba8a4a8yb9bb92b8y9ya8ayyb9y884b992a2a0a1a0a2a2a4ay4b80b8y00rj2am0ttnuls201aohap2cv , abgerufen am 17.07.2024).

[22] Diese Adressaten werden aber nicht immer in den bauaufsichtlichen Maßnahmen erwähnt: *Kaiser*, § 41 Bauordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, [4]2020, Rn. 145. Siehe a.: § 80 MBO.

[23] Dazu: Kapitel 5 G. Herstellerverantwortlichkeit.

von Soft- und Hardware oder den Infrastrukturanbieter[24]. Je nach konkreter Verantwortlichkeitsform ließen sich dann die datenschutzrechtlichen Pflichten einschränken bzw. erweitern oder Privilegien vergeben. Die Schwierigkeit einer solchen Typologie dürfte allerdings darin liegen, überhaupt relevante Beteiligungsformen zu erfassen, da die Beteiligungsformen an einer Verarbeitung extrem vielfältig sind. Dies gilt gerade auch im Hinblick auf die Beteiligung an verschiedenen Verarbeitungsvorgängen. Trotzdem dürfte es möglich sein, langfristig im Rahmen von aufsichtsbehördlichen Gremien sowie durch Interessensverbände konsistent auftretende Verantwortlichkeitsformen zu erfassen und zu abstrahieren. Diese könnten dann jedenfalls im Rahmen von Leitlinien der Aufsichtsbehörden berücksichtigt werden und langfristig in Reformen der DSGVO einbezogen werden.

C. „Datenschutzrechtliche Gesamtschuldnerschaft"

Einen eher radikalen Ansatz stellt die „datenschutzrechtliche Gesamtschuldnerschaft"[25] dar. Ausgangspunkt hierfür ist die Annahme, dass Verarbeitungen in umfassend vernetzten Strukturen sowie transnational erfolgen.[26] Zudem seien Verarbeitungsschritte nicht mehr im Detail nachvollziehbar. Konsequenz soll daher eine gänzlich neue Form der Zuordnung datenschutzrechtlicher Verantwortung sein. Diese Verantwortung soll natürliche oder juristische Personen treffen, die personenbezogene Daten zur Aufgabenerfüllung[27] erstmals direkt bei der betroffenen Person erheben oder aus anderen Quellen zu Dateien zusammenfügen. Einer solchen Stelle[28] soll es dann in eigener Verantwortung obliegen „für alle Verarbeitungsschritte, die sie ermöglicht oder veranlasst, gesetzeskonforme Zustände zu realisieren und zu garantieren"[29]. Weitere Voraussetzung dieser „datenschutzrechtlichen Gesamtschuldnerschaft" sollen aber auch größere Spielräume für die durchzuführenden Verarbeitungen sein. Schließlich sollen

[24] Dazu: Kapitel 5 H. Intermediärsverantwortlichkeit.

[25] *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 79.

[26] Dabei wird insb. auf „ubiquitous computing" hingewiesen.

[27] Sinnvollerweise scheint hier eine Zweckerfüllung gemeint, da sonst eine Reduktion auf die Verarbeitungsrechtfertigung aus Art. 6 Abs. 1 lit. e DSGVO naheliegt.

[28] Ironischerweise will der Verfasser kurz vorher vom Begriff der „Stelle" als Anknüpfungspunkt für Verantwortlichkeiten Abschied nehmen.

[29] *Wedde*, 4.3 Verantwortliche Stellen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 79.

Verstöße gegen gesetzliche Vorgaben durch hohe Konventionalstrafen geahndet werden, die zudem verschuldensunabhängig anfallen sollen. Hierbei handelt es sich um einen Vorschlag nach noch zu schaffendem Recht.

Ob dieser Vorschlag tatsächlich umsetzbar ist, stellt selbst dessen Urheber in Frage.[30] Daneben ist bestenfalls unklar, inwiefern eine verschuldensunabhängige Bußgeldhaftung zumindest mit dem unionsrechtlichen Sanktionsrecht vereinbar ist.[31] Vor allem aber scheint der Fokus auf den Ersterheber bzw. -verarbeiter nicht zielgerecht. Dieser Ansatz mag möglicherweise dem Prinzip der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO im Sinne eines Anreizes zur Datenvermeidung dienen, verliert aber die Auswirkungen der konkreten Verarbeitung aus dem Fokus. Sinn des Datenschutzes ist ausweislich des sogenannten „Verbotsgrundsatzes" aus Art. 5 Abs. 1 lit. a DSGVO allerdings nicht die Verhinderung von Datenverarbeitungen überhaupt, sondern deren rechtliche Einhegung durch Verarbeitungsrechtfertigungen. Schließlich bietet die „datenschutzrechtliche Gesamtschuldnerschaft" auch keinerlei praktikable Ansätze für Verarbeitungsszenarien mit mehreren Akteuren. So stellt sich etwa die Frage, ob der Zweitverarbeiter ebenso wie der Erstverarbeiter für einen Drittverarbeiter mitverantwortlich wäre.[32] Insgesamt scheint der Ansatz in der vorgeschlagenen Form daher nicht zielführend.

D. Anwendung der DSA-Privilegierungen[33]

Unabhängig von der Frage, wie sich der DSA zur DSGVO[34] verhält, scheint die Anwendung der Privilegierungen aus dem DSA erwägenswert.[35] Da bislang davon auszugehen ist, dass die Privilegierungen des DSA insgesamt keine Anwendung auf die DSGVO finden, wäre dies ein Ansatz nach noch zu schaffendem Recht. Die Konse-

[30] Zudem liegt er mindestens 19 Jahre zurück und erfolgte noch zum BDSG a.F.

[31] EuGH, Urteil vom 05.12.2023 – C-807/21 (Deutsche Wohnen) = ZD 2024, 203.

[32] Wie in langen Verarbeitungsketten dann die Mitverantwortlichkeiten zu dokumentieren wären, ist eine weitere Frage. Denkbar wäre eine Art Blockchain der Verantwortlichkeit.

[33] In der Abgabeversion dieser Arbeit wurde noch die e-Commerce-RL behandelt. Allerdings wurden durch Art. 89 Abs. 1 DSA die Art. 12-15 e-Commerce-RL gestrichen. Maßgeblich sind nun gem. Art. 89 Abs. 2 DSA die Art. 4, 5, 6 und 8 DSA. Die notwendigen Anpassungen wurden vorgenommen, allerdings beziehen sich weite Teile der Literatur noch auf die e-Commerce-RL.

[34] Dazu: Kapitel 3 B. Das Verhältnis von DSGVO und e-Commerce-RL bzw. DSA.

[35] Vgl. a. *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 875 ff.

quenzen einer Anwendung dieser Privilegierungen lassen sich im Rahmen einer Entscheidung des höchsten italienischen Gerichts,[36] der Corte di Cassazione, darstellen. In diesem Verfahren hatte das Gericht trotz der Regelung des Anwendungsbereichs in Art. 1 Abs. 5 lit. b e-Commerce-RL[37] die Privilegierungen der e-Commerce-RL auf einen datenschutzrechtlichen Sachverhalt angewandt. Konkret ging es in dem Verfahren um Betroffenenrechte im Hinblick auf ein Video, das von Google gehostet wurde. Folge der Anwendung der Privilegierungen e-Commerce-RL war nach Ansicht des Gerichts, dass Google vor dem Inkenntnissetzen durch die betroffene Person gem. Art. 14 Abs. 1 lit. b e-Commerce-RL[38] nicht datenschutzrechtlich verantwortlich war. Dabei hielt das Gericht fest, dass der Online-Service-Provider (OSP) als Anbieter eines Dienstes der Informationsgesellschaft zunächst kein Verantwortlicher für die Verarbeitung sei, sondern nur der Nutzer, der den Inhalt, also das Video, gepostet hatte. Der OSP werde erst durch das Inkenntnissetzen der betroffenen Person zum Verantwortlichen, denn der Hoster habe ohne Kenntnis von der Verarbeitung keine Entscheidungsmacht über diese.[39]

Für Host-Provider gem. Art. 6 DSA stellt sich nach dem Inkenntnissetzen durch die betroffene Person dann allerdings die Frage, ob sie den maßgeblichen Inhalt nach den Verfahrensvorgaben[40] der DSGVO oder des DSA entfernen müssten.[41] Daneben ließ die Begründung des Gerichts außer Acht, dass bestimmte Host-Provider sehr wohl im Rahmen gewisser Verarbeitungsvorgänge über die Zwecke und Mittel der Verarbeitung, mangels einer Auftragsverarbeitung,[42] entscheiden. Dies gilt vor allem für Plattformen mit user-generated content. Zu denken ist dabei etwa an die Darstellung des Inhaltsfeeds eines Nutzers, die Rangfolge von Suchergebnissen oder an Prüfsysteme hinsichtlich bestimmter Inhalte, die entweder durch Algorithmen des Host-Providers oder diesen selbst determiniert werden. Neben dieser Privilegierung des Host-Providers würden auch die Privilegierungen gem. Art. 4 DSA für die reine Durchleitung sowie gem. Art. 5 DSA für das Caching greifen. Die entsprechenden Anbieter von Diensten der Informationsgesellschaft wären dann unter den jeweiligen Voraussetzungen nicht nur von einer Haftung, etwa auf Unterlassung oder Schadensersatz, freigestellt, sondern überhaupt nicht verantwortlich.

---

[36] Corte di Cassazione, Cass. sez. tre Penale, 3 febbraio 2014, n. 5107/14 (It.).

[37] Mittlerweile Art. 2 Abs. 4 lit. g DSA.

[38] Mittlerweile Art. 6 Abs. 1 lit. b DSA.

[39] Vgl. die Übersetzung bei *Keller*, BTLJ[33] (2018), 287, 359. Vgl. a. Kapitel 2. E. I. Vorfrage: Notwendige Kenntniselemente der Entscheidung.

[40] Also welches notice-and-take-down-Verfahren gilt.

[41] *Keller*, BTLJ[33] (2018), 287, 359.

[42] So a.: *Keller*, BTLJ[33] (2018), 287, 360; vgl. *Sartor*, MJ[21] (2014), 564, 575.

Statt dieser pauschalen Anwendung der Privilegierungen des DSA schlägt *Keller* vor, nur die Verfahrensregeln hinsichtlich des notice-and-take-down-Verfahrens, basierend auf der Rechtsprechung zur e-Commerce-RL, auf das Verfahren für das Recht auf Vergessenwerden nach Art. 17 Abs. 2 DSGVO anzuwenden.[43] Dies sei mit Art. 2 Abs. 4 DSGVO vereinbar. Alternativ könnten Host-Provider aber auch generell von dem Betroffenenrecht gem. Art. 17 Abs. 2 DSGVO freigestellt werden.[44] Dabei müssten dann allerdings andere Verfahrensregeln als für Suchmaschinenbetreiber greifen. Denn Host-Provider seien häufig die Quelle für die Ergebnisse der Suchmaschinenbetreiber. *Sartor* betont neben dem Abs. 1 von Art. 14 e-Commerce-RL auch dessen Abs. 3,[45] gemäß dem ein Gericht oder eine Verwaltungsbehörde nach dem Recht der Mitgliedstaaten von einem Diensteanbieter verlangen kann, eine Rechtsverletzung abzustellen oder zu verhindern.[46] Eine datenschutzrechtliche Aufsichtsbehörde solle demnach unproblematisch Ansprüche nach Art. 17 Abs. 2 DSGVO durchsetzen können. Einer betroffenen Person selbst solle die Durchsetzung eines solchen Anspruchs hingegen nur gelingen, sofern neben der Inkenntnissetzung (als empirischem Aspekt) des Host-Providers auch eine eindeutige Illegalität (als rechtlichem Aspekt) des streitigen Verstoßes gegeben sei.[47] Diese eindeutige Illegalität solle sich aus rechtlichen Quellen, maßgeblichen Entscheidungen oder rechtlicher Offensichtlichkeit ergeben. Je nach Verhalten des Host-Providers in Reaktion auf das Inkenntnissetzen durch die betroffene Person seien verschiedene Grade der Haftung denkbar.[48] *Van Alsenoy* schließlich möchte die (vermeintliche)[49] Anwendung der e-Commerce-Privilegierungen auf die DSGVO gem. Art. 2 Abs. 4 DSGVO so verstehen, dass nur die Haftung auf Schadensersatz, und vermutlich auch auf Geldbußen, unter den Voraussetzungen der jeweiligen Privilegierungen entfalle.[50] Dieses Verständnis decke sich auch mit der Rechtsprechung des EuGH im Urteil zu Google Spain.

Vorteil einer Anwendung der Privilegierungen aus dem DSA wäre sicherlich eine einheitliche Behandlung der Haftungsfragen von Intermediären.[51] Allerdings sind die von dem DSA in Art. 4 - 6 erfassten Rechtssubjekte keinesfalls unproblematisch in ihrer

[43] *Keller*, BTLJ[33] (2018), 287, 361.
[44] *Keller*, BTLJ[33] (2018), 287, 362 f.
[45] Entsprechend Art. 6 Abs. 1 und 4 DSA.
[46] *Sartor*, MJ[21] (2014), 564, 571 ff.
[47] Vgl. das Google Spain Beispiel *Sartor*, MJ[21] (2014), 564, 573.
[48] *Sartor*, MJ[21] (2014), 564, 572 f.
[49] Dazu: Kapitel 3 B. Das Verhältnis von DSGVO und e-Commerce-RL bzw. DSA.
[50] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 46.
[51] *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1252, siehe a.: *Keller*, BTLJ[33] (2018), 287, 351 ff.

Abgrenzung.[52] Auch Mischformen werden nur unzureichend von dem DSA erfasst, wie etwa Art. 21 Abs. 2 e-Commerce-RL für Suchmaschinen verdeutlicht. Daneben wären nur sehr spezifische Verarbeitungsvorgänge privilegiert.[53] Sinnvoll erscheint eine Anwendung der Privilegierungen, insbesondere von Art. 6 DSA, hinsichtlich der Wahrung anderer Grundrechte wie der Meinungs- oder der Informationsfreiheit.[54] Hierfür ist aber wiederum nicht eine vollständige Entbindung von sämtlichen Pflichten eines Verantwortlichen notwendig. Maßgeblich bleibt zudem vor allem die Frage, was genau die Privilegierungen nach Art. 4 - 6 DSA in ihrer Anwendung auf die DSGVO erfassen sollen. Denkbar ist es nur auf die Haftung im engeren Sinne, also für Schäden, abzustellen.[55] Gleichermaßen könnten damit aber auch die Verantwortlichkeit und die daran anknüpfenden Verpflichtungen erfasst sein. Sinnvollerweise sollte nur die Haftung im engeren Sinne, also Schadenersatz und ggf. Geldbußen durch die Privilegierungen ausgenommen sein. Eine Anwendung der Privilegierungen der DSA auf die Verantwortlichkeit als solche würde nicht zu einer transparenteren Verteilung der Verantwortlichkeit zwischen den Nutzern der privilegierten Dienste und deren Anbietern führen. So lässt sich aus den Privilegierungen der Art. 4 - 6 DSA keine weitere Art der Verantwortlichkeit neben der des Verantwortlichen begründen, da diese Privilegierungen eine anderweitig bereits bestehende Verantwortlichkeit voraussetzen.[56] Aus Sicht der betroffenen Personen würde eine Anwendung der Privilegierungen vielmehr zu einer faktischen Verschlechterung führen. Geht man davon aus, dass die Haushaltsausnahme in Art. 2 Abs. 2 lit. c DSGVO für die Nutzer von Plattformen wie z.B. sozialen Netzen gilt,[57] würde eine Anwendung von Art. 6 DSA grundsätzlich eine weitere Verzögerung der Durchsetzung der Rechte betroffener Personen bedeuten. Denn weder der Nutzer, der den Inhalt gepostet oder hochgeladen hat, noch der Anbieter der Plattform wären dann unmittelbar nach der DSGVO zur Löschung verpflichtet. Denkbar sind zwar grundsätzlich Löschungsansprüche aus anderen Rechtsgebieten, wie dem Äußerungsrecht, aber auch solche Ansprüche müssen nicht immer zwingend bestehen. Der von *Sartor* vorgeschlagene Umweg der Löschung über die Aufsichtsbehörden dürfte im Hinblick auf deren knappe Ausstattung kaum eine praktikable Alternative darstellen.

[52] Siehe a.: *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1253.
[53] *Alsenoy*, JIPITEC[7] (2016), 271, Rn. 46.
[54] Siehe: *Sartor*, IDPL[3] (2013), 3, 4.
[55] Vgl. *Alsenoy*, Regulating Data Protection, 08.2016, Rn. 1262.
[56] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 11.
[57] Dazu: Kapitel 5 I. Haushaltsausnahme.

Insgesamt trägt die Anwendung der Privilegierungen aus der DSA im Rahmen der DSGVO nicht dazu bei, die Defizite des Konzeptes der Verantwortlichkeit zu kompensieren. Abseits des teilweise immer noch unklaren Verhältnisses des DSA zur DSGVO bestehen eine Reihe von Folgefragen, die nur de lege ferenda zu klären sind.

E. Auswahlverantwortlichkeit

Im Vorfeld des Urteils des EuGH in der Rechtssache Wirtschaftsakademie[58] hatte das BVerwG in seinem Vorlagebeschluss eine allgemeine Auswahlverantwortlichkeit erwogen.[59] Das BVerwG stellte sich hierbei die Frage, ob der Rechtsgedanke der Auswahlverantwortlichkeit des Verantwortlichen nach Art. 17 Abs. 2 DSRL[60] nur auf die Auftragsverarbeitung beschränkt sei oder für die DSRL in analoger Anwendung verallgemeinbar wäre, gegebenenfalls nach Recht eines Mitgliedstaates.[61] Dieser Ansatz wäre, ohne richterliche Rechtsfortbildung, als de lege ferenda zu verstehen. Grundgedanke des Ansatzes ist, „[...] dass sich ein Informationsanbieter nicht durch die Wahl eines bestimmten Infrastrukturanbieters von datenschutzschutzrechtlichen Pflichten im Verhältnis zu den Nutzern seines Informationsangebotes soll freizeichnen dürfen, die er bei einem reinen Content-Provider zu erfüllen hätte."[62] Das BVerwG kam im Vorlagebeschluss zu der Rechtssache Wirtschaftsakademie zu dem Schluss, dass dem Sachverhalt eine spezifische Gefährdungslage zugrunde liege, die nicht von der Definition des Verantwortlichen in Art. 2 lit. d DSRL[63] erfasst sei. Dies wurde damit begründet, dass der Fanpage-Betreiber als Informationsanbieter gleichzeitig auch Nutzer des sozialen Netzwerks des Plattformbetreibers sei und die Verantwortungsverteilung für die Nutzer des Informationsangebotes nicht hinreichend klar wäre.[64] Der EuGH setzte sich

[58] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[59] BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 438: „2. Folgt aus der Pflicht der Mitgliedstaaten nach Art. 17 Abs. 2 RL 95/46/EG, bei der Datenverarbeitung im Auftrag vorzuschreiben, dass der für die Verarbeitung Verantwortliche einen „Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichend Gewähr bietet", im Umkehrschluss, dass bei anderen Nutzungsverhältnissen, die nicht mit einer Datenverarbeitung im Auftrag im Sinne des Art. 2 Buchst. e) RL 95/46/EG verbunden sind, keine Pflicht zur sorgfältigen Auswahl besteht und auch nach nationalem Recht nicht begründet werden kann?"

[60] Mittlerweile Art. 28 Abs. 1 DSGVO.

[61] Detailliert: *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 11 ff.

[62] BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 440 Rn. 35.

[63] Mittlerweile Art. 4 Nr. 7 DSGVO.

[64] Unter anderem a. deswegen, da sich das Informationsangebot a. an Nutzer außerhalb des sozialen Netzwerkes richtete.

mit diesem Ansatz in der Rechtssache Wirtschaftsakademie nicht weiter auseinander, da er eine gemeinsame Verantwortlichkeit des Fanpage-Betreibers und des Plattformbetreibers feststellte. Konzeptionell kann man die Auswahlverantwortlichkeit als Konsequenz der Ermöglichung der Datenverarbeitung eines Dritten unter der Vermeidung einer eigenen Verantwortlichkeit verstehen. Diese eigene Verantwortlichkeit würde im Rahmen einer eigenen Durchführung der Verarbeitung bzw. einer eigenen Bereitstellung eines entsprechenden Angebotes vorliegen.

Der Ansatz einer Auswahlverantwortlichkeit erscheint grundsätzlich als ein angemessener Mittelweg zwischen einer regulären Verantwortlichkeit und der Nichterfassung eines Akteurs, der nur geringfügige Beiträge zu einer Verarbeitung leistet. Durch das Urteil des EuGH in der Rechtssache Wirtschaftsakademie besteht aber aufgrund der gemeinsamen Verantwortlichkeit eines Fanpage-Betreibers und des Plattformbetreibers eines sozialen Netzwerks mangels planwidriger Regelungslücke kein Raum für eine solche Analogie.[65] Dies gilt jedenfalls solange, wie die Grenzen des notwendigen Entscheidungsbeitrags eines gemeinsam Verantwortlichen nicht ausgelotet sind und daher kein Bedarf für eine solche Auswahlverantwortlichkeit besteht. Darüber hinaus setzt die Auswahlverantwortlichkeit im Grunde genommen auch zwei Analogien voraus. Denn zum einen müsste die Auswahlverantwortlichkeit aus Art. 28 Abs. 1 DSGVO für Verhältnisse mehrerer Akteure außerhalb einer Auftragsverarbeitung gelten, etwa für die Übermittlung zwischen zwei Verantwortlichen. Zum anderen müsste eine völlig neue datenschutzrechtliche Verantwortlichkeitsrolle im Rahmen dieser Analogie gebildet werden. Bestünde bereits eine datenschutzrechtliche Verantwortlichkeit des Auswahlverantwortlichen wäre diese schließlich mangels Regelungslücke nicht nötig. Die Auswahlverantwortlichkeit schafft also nicht nur eine zusätzliche Pflicht, die de lege lata nur für Verantwortliche im Rahmen ihrer Rolle als Auftraggeber besteht, sondern setzt gleichzeitig eine weder definierte noch systematisch vorausgesetzte Rolle voraus. Insbesondere wären zunächst die spezifischen Pflichten, die mit so einer Auswahlverantwortlichkeit verbunden sind zu klären. Auch wenn ein dringender Bedarf für eine Rolle zwischen Verantwortlichkeit und Nicht-Verantwortlichkeit besteht, lässt sich diese nicht de lege lata nicht mit einer Auswahlverantwortlichkeit füllen. De lege ferenda wäre sie zwar wünschenswert, sie wäre dann aber auch von einer „datenschutzrechtlichen Beihilfe“[66] abzugrenzen.

[65] Vgl. BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 440 Rn. 36.

[66] Dazu: Kapitel 5 F. „Datenschutzrechtliche Beihilfe“.

F. „Datenschutzrechtliche Beihilfe“

Ein weiterer naheliegender Ansatz für eine Ergänzung der Verantwortlichkeitsrollen wäre de lege ferenda die Einführung einer Art „datenschutzrechtlichen Beihilfe“.[67] In dem Ausmaß des Beitrags zu einer Verarbeitung wäre die datenschutzrechtliche Beihilfe zwischen dem Verantwortlichen und dem Auftragsverarbeiter anzusetzen.[68] Die Pflichten des datenschutzrechtlichen Gehilfen wäre konsequenterweise gegenüber dem Auftragsverarbeiter zumindest leicht erhöht. Eine Privilegierung hinsichtlich der Verarbeitungsrechtfertigung wäre aber jedenfalls abzulehnen. Gegenüber dem Auftragsverarbeiter würde sich der datenschutzrechtliche Gehilfe dadurch abgrenzen, dass er keiner Weisungsgebundenheit unterliegt. Gegenüber dem Verantwortlichen wiederum würde er sich dadurch abgrenzen, dass er weder über die Zwecke noch insgesamt über die Mittel entscheidet, sondern nur über unwesentliche Elemente[69] der Mittel. Eine Verantwortlichkeit im Sinne von Art. 4 Nr. 7 DSGVO wäre also erst dann anzunehmen, wenn der maßgebliche Akteur entweder über wesentliche Elemente der Mittel oder die Zwecke entscheidet. Insofern wäre die datenschutzrechtliche Beihilfe mit dem Auftragsverarbeiterexzess gem. Art. 28 Abs. 10 DSGVO und insgesamt der Verantwortlichkeitssystematik kompatibel. Man kann den datenschutzrechtlichen Gehilfen insgesamt als einen Auftragsverarbeiter ohne Weisungsgebundenheit verstehen.

Sinnvoll erscheint die datenschutzrechtliche Beihilfe vor allem in Ergänzung zu einer Auswahlverantwortlichkeit.[70] Während die Auswahlverantwortlichkeit auf die Ermöglichung einer fremden Verarbeitung abstellen würde, würde die datenschutzrechtliche Beihilfe geringfügige Entscheidungsbeiträge zu den Mitteln einer Verarbeitung eines anderen Verantwortlichen berücksichtigen. Der Kontrollverlust gegenüber einem Auftragsverarbeiter wäre dabei dadurch kompensiert, dass die Pflichten für den datenschutzrechtlichen Gehilfen entsprechend seines Beitrags zu den Mitteln ausgeweitet wären. Zu denken wäre dabei insbesondere an die Pflichten aus Art. 25 und 32 DSGVO. Daneben wäre auch eine flexiblere Haftung im Vergleich zur eingeschränkten Haftung des Auftragsverarbeiters gem. Art. 82 Abs. 2 S. 2 DSGVO notwendig. Naheliegend wäre zudem die eingeschränkte Möglichkeit der Verhängung von Geldbußen gem. Art. 83 DSGVO gegenüber dem datenschutzrechtlichen Gehilfen. Im Gegenzug

[67] Dazu: Kapitel 4 I. II. Qualitative Einschränkungen im Hinblick auf die Erheblichkeitsschwelle.

[68] Es ginge also nicht um eine Art „Mittäterschaft“, vgl. *Weichert*, ZD 2014, 605, 610. Vgl. zum Begriff *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 8.

[69] Dazu: Kapitel 2 D. Mittel.

[70] Dazu: Kapitel 5 E. Auswahlverantwortlichkeit.

würden einen „Auftragsverarbeiter ohne Weisungsabhängigkeit“ aber nicht die umfassenden Pflichten und die Haftung einer regulären Verantwortlichkeit treffen. Zusammen mit der Auswahlverantwortlichkeit ließe sich so die gemeinsame Verantwortlichkeit entzerren und Grenzfälle ließen sich besser fassen. Dies würde insgesamt die gemeinsame Verantwortlichkeit als Konzept stabilisieren.[71]

G. Herstellerverantwortlichkeit

Neben diesen eher allgemeineren Ansätzen zur Verantwortlichkeit gibt es auch Ansätze, die an spezifische Pflichten der DSGVO oder spezifische Verarbeitungsszenarien anknüpfen. Die Herstellerverantwortlichkeit setzt an die Regelungen zum Datenschutz durch Technik an.[72] Es handelt sich hierbei um einen Ansatz nach noch zu schaffendem Recht. Zwar regelt Art. 25 DSGVO ganz allgemein den Datenschutz durch Technikgestaltung (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default). Dabei wird allerdings nur der Verantwortliche gem. Art. 4 Nr. 7 DSGVO als Adressat angesprochen.[73] Mittelbar wird zudem der Auftragsverarbeiter gem. Art. 28 DSGVO erfasst, da der Verantwortliche gem. Art. 28 Abs. 1 DSGVO die Verantwortung dafür trägt, dass er Auftragsverarbeiter auswählt, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden. Im Gesetzgebungsverfahren zur DSGVO wurde allerdings auch diskutiert, ob Art. 25 Abs. 1 DSGVO für Hersteller von Hard- und Software[74] unmittelbar gelten sollte.[75] Bereits im Vorfeld des Gesetzgebungsverfahrens hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder noch auf

[71] Zu potenziellen Anwendungsfällen: Kapitel 4 I. II. Qualitative Einschränkungen im Hinblick auf die Erheblichkeitsschwelle.

[72] Vgl. a. die Verantwortlichkeit von Plattformbetreibern bei *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 267 ff.

[73] Sydow/Marsch/*Mantz*, Art. 25 DSGVO, Rn. 16, 65 ff.; Simitis/Hornung/Spiecker/*Hansen*, Art. 25 DSGVO, Rn. 21; Kuner/Bygrave/Docksey/*Bygrave*, Art. 25 GDPR, 578.

[74] Insgesamt in den Änderungsanträgen als automatische Datenverarbeitungssysteme bezeichnet.

[75] *Albrecht* Berichtsentwurf v. 16.01.2013 2012/0011(COD), Änderungsantrag 88, 98, unklar: 178. Ebenso: EDPS Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union" v. 14.01.2011, Rn. 112. Bereits vorab: *Artikel-29-Datenschutzgruppe*, Die Zukunft des Datenschutzes, 01.12.2009, Rn. 46, 51.

die mangelnde Berücksichtigung von Herstellern sowie Entwicklern von Produkten und Verfahren hingewiesen.[76]

Von der Herstellerverantwortlichkeit sind wiederum Akteure abzugrenzen, die neben Soft- oder Hardware auch eine Dienstleistung diesbezüglich, etwa das Hosting anbieten. Hintergrund der Überlegungen zu einer Herstellerverantwortlichkeit war, dass vielfach von Verantwortlichen fertige (Standard-)Soft- und/oder Hardware eingesetzt wird. Dabei haben die Verantwortlichen insbesondere bei Standardprodukten so gut wie keinen Einfluss auf die Gestaltung der Datenverarbeitung.[77] Daher wird für einen wirksamen Datenschutz durch Technik gefordert, dass auch Hersteller in Art. 25 DSGVO einbezogen werden sollten.[78] Diese Forderung hat sich aber letztlich im Gesetzgebungsverfahren nicht durchsetzen können, so dass nach momentaner Rechtslage allenfalls mittelbar ein Anreiz für die Hersteller von Soft- und Hardware zur Datenschutzkonformität besteht.[79] Bislang lässt nur ErwGr 78 S. 4 DSGVO explizit einen Appell an die Hersteller erkennen:

> *„In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen."*

Dieser Erwägungsgrund wird aufgrund der mangelnden Verpflichtung der Hersteller (und damit einhergehend auch der mangelnden Bußgeldbewehrung) als wohlgemeinter Programmsatz kritisiert.[80] Ein Datenschutz durch Technikgestaltung sei ohne

---

[76] *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 18.03.2010, 7 f.

[77] Vgl. aber zu Standardisierungsgremien wie W3C Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 151.

[78] Vgl. etwa *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 117 f. Sydow/Marsch/*Mantz*, Art. 25 DSGVO, Rn. 17 m.w.N.

[79] Dazu eingehender: Sydow/Marsch/*Mantz*, Art. 25 DSGVO, Rn. 78 ff. Optimistisch im Hinblick auf eine indirekte Wirkung: Ehmann/Selmayr/*Baumgartner*, Art. 25 DS-GVO, Rn. 12. Kritisch: *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 90; Taeger/Gabel/*Lang*, Art. 25 DSGVO, Rn. 26 ff.

[80] *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht,

die Ausweitung des Adressatenkreises auf die Hersteller nur bedingt wirkungsvoll.[81] Folglich müsse eine weitere Verpflichtung der Hersteller auf mitgliedstaatlicher Ebene, idealerweise aber durch den Unionsgesetzgeber erfolgen.

Auch über Umwege lässt sich eine Verantwortlichkeit von reinen Herstellern nicht konstruieren. Mangels Weisungsgebundenheit der Hersteller besteht regelmäßig keine Auftragsverarbeitung durch den bloßen Einsatz von Soft- oder Hardware seitens der Nutzer, selbst wenn man von einer Entscheidung über bestimmte Elemente der Mittel ausgeht. Ebenso liegt auch keine singuläre Verantwortlichkeit vor, da Hersteller mit der Produktion von Soft- oder Hardware nicht über die Zwecke der Verarbeitung entscheiden. Eine gemeinsame Verantwortlichkeit liegt gleichermaßen fern. Zwar liegen durch die zur Verfügung gestellte Soft- oder Hardware hinsichtlich der Technik durchaus gemeinsame Mittel im technischen Sinne vor, allerdings fehlt für gemeinsame Mittel dann noch die Identität der Verarbeitung anhand der verarbeiteten Daten. Auch die Anwendung der DSA-Privilegierungen wäre nicht weiterführend, da reine Hersteller keine Dienste im Sinne von Art. 4 - 6 DSA anbieten. Die Auswahlverantwortlichkeit wiederum wäre schwerpunktmäßig auf die Erbringung von Dienstleistungen im Zusammenhang mit Verarbeitungen zu verstehen, weniger als bloße Bereitstellung von Soft- oder Hardware. Die datenschutzrechtliche Beihilfe schließlich würde ebenso wie die gemeinsame Verantwortlichkeit an der Identität der Verarbeitung scheitern.

I. Frühere Ansätze

Die Idee einer Herstellerverantwortlichkeit ist in etwa so alt wie der Datenschutz in Deutschland überhaupt. So wurde bereits im Steinmüller-Gutachten von 1971 festgehalten, dass Programme, in denen konkrete Austauschvorgänge geregelt sind, (zumindest auch in Teilen) Normcharakter besitzen.[82] Sie sollten veröffentlicht werden,[83] bedürften einer aufsichtlichen Genehmigung und unterlägen gerichtlicher Nachprüfung. Überwacht werden sollte dies durch ein (Bundes-/Landes-)Informationsamt bzw. einen -hof. Auch die technische Organisation eines Informationssystems sollte genehmigungspflichtig sein. Dabei sollten auf das Informationssystem zugeschnittene individuelle Auflagen gemacht werden können.[84] Zwar ist einzuräumen, dass man 1971 von gänzlich anderen technischen Voraussetzungen ausging. Trotzdem ist ein Ansatz zur

26.11.2019, 50 f.

[81] *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 51, 90.

[82] BT-Drs. VI/3826, S. 129.

[83] Etwa in Form von zu standardisierenden Programmbeschreibungen.

[84] BT-Drs. VI/3826, S. 152 f.

Verantwortlichkeit nicht nur beim Verwender der Technik, sondern auch der verwendeten Technik selbst deutlich erkennbar. Ebenso wurde im 2001 veröffentlichten Gutachten zur „Modernisierung des Datenschutzrechts" im Auftrag des BMI eine Verpflichtung der Hersteller gefordert, für die Gestaltung ihrer Produkte zumindest die Erfüllung einiger zentraler Produktanforderungen zu überprüfen.[85] Anforderungen an Datenschutz und Datensicherheit sollten also bereits in der Entwicklung und Herstellung von Produkten berücksichtigt werden. Dafür sollten per Gesetz materielle Anforderungen im Wege von Prüfpflichten formuliert werden. Die Verletzung dieser Prüfpflichten sollte eine Sorgfaltspflichtverletzung darstellen. Die Prüfpflichten sollten zudem zusätzlich durch Dokumentationspflichten sowie Verwendungsempfehlungen der Hersteller flankiert werden. Begründet wurden diese Forderungen damit, dass viele Gestaltungsanforderungen des Datenschutzrechts vom Verantwortlichen gar nicht erfüllt werden könnten. Diesen fehle meist das technische Wissen, die Gestaltungskompetenz und vor allem der Zugriff auf Soft- und Hardware.[86]

II. Konkrete Regelungsvorschläge

1. BDSG a.F.

Die Autoren des BMI-Gutachtens formulierten dabei folgenden Vorschlag für eine Regelung:[87]

> *„(1) Hersteller haben bei Entwicklung und Herstellung von Produkten der Informationstechnik (Hardware, Software und automatisierte Verfahren) zu prüfen, ob und wie es möglich ist,*
>
> > *1. die Verarbeitung personenbezogener Daten zu vermeiden oder zu vermindern,*
> > *2. die Transparenz über die Funktionen und die Verarbeitung personenbezogener Daten für den Nutzer herzustellen oder zu erhöhen,*
> > *3. werkseitig die für den Nutzer datenschutzfördernde und sichere Voreinstellung zu wählen,*

[85] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 17, 36, 143 ff.
[86] *Roßnagel*, MMR 2005, 71, 74 f.
[87] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 143 f.

4. die Möglichkeiten des Nutzers zur Kontrolle über die Verarbeitung personenbezogener Daten und Sicherheitseigenschaften zu schaffen oder zu verbessern,
5. die Verwendung von Funktionen und personenbezogenen Daten für nicht vorgesehene Zwecke zu verhindern oder zumindest zu erschweren,
6. personenbezogene Daten für unterschiedliche Zwecke getrennt zu verarbeiten,
7. die sichere und datenschutzgerechte oder datenschutzfördernde Verwendung der Produkte zu kontrollieren.

Die Ergebnisse der Prüfung sind bei der Entwicklung und Herstellung von Produkten der Informationstechnik zu berücksichtigen.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die Produkte der Informationstechnik zu bestimmen, bei deren Entwicklung und Herstellung die Prüfung nach Absatz 1 zu dokumentieren ist.

(3) Hersteller und Vertreiber von Produkten der Informationstechnik weisen in geeigneter Weise auf Risiken und förderliche Eigenschaften für Datenschutz und Datensicherheit hin und geben Empfehlungen zu ihrer datenschutzgerechten oder datenschutzfördernden und sicheren Verwendung."

2. DSGVO

Die Änderungsanträge für den Kommissionsentwurf der DSGVO verfolgten hingegen einen anderen Ansatz.[88] So sollte der Begriff des Herstellers definiert werden und dieser Hersteller auf die Einhaltung der Grundsätze des Art. 5 DSGVO sowie zu Maßnahmen verpflichtet werden, um sicherzustellen, dass seine Produkte den Verantwortlichen die Erfüllung derer Pflichten nach Art. 25 DSGVO ermöglichen. Daher sollte nach Änderungsantrag 88 des Albrecht-Berichtsentwurfs die Definition des Herstellers in Art. 4 wie folgt lauten:

„‚Hersteller' eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Systeme für die automatische Verarbeitung von personen-

[88] *Albrecht* Berichtsentwurf v. 16.01.2013 2012/0011(COD), Änderungsantrag 88, 98, 178.

bezogenen Daten oder Ablagesysteme für die Verarbeitung von personenbezogenen Daten durch die für die Verarbeitung Verantwortlichen und für die Auftragsverarbeiter herstellt;"

Ebenso sollte Art. 5 nach Änderungsantrag 98 wie folgt ergänzt werden:

„Die Verarbeitung personenbezogener Daten ist in einer Weise zu organisieren und durchzuführen, die die Einhaltung der Grundsätze des Absatzes 1 sicherstellt; Hersteller, für die Verarbeitung Verantwortliche und Auftragsverarbeiter ergreifen technische und operationelle Maßnahmen, um diese Einhaltung bei der Planung, Einrichtung und Anwendung von Systemen für die automatische Datenverarbeitung oder von Ablagesystemen sicherzustellen."

Dies sollte ausweislich der Begründung insbesondere für weitverbreitete Standardanwendungen, aber auch für Nischenprodukte gelten.

Schließlich sollte Änderungsantrag 178 den heutigen Art. 25 DSGVO wie folgt ergänzen:

„Datenverarbeiter und -produzenten führen technische und organisatorische Maßnahmen und Verfahren durch, mit denen sichergestellt wird, dass ihre Dienste und Produkte es den für die Verarbeitung Verantwortlichen durch Voreinstellungen erlauben, die Auflagen dieser Verordnung zu erfüllen, insbesondere, was die in den Absätzen 1 und 2 erwähnten Auflagen betrifft."

Bei den Begriffen der Datenverarbeiter und -produzenten handelt es sich um einen Übersetzungsfehler. Ausweislich der englischen Sprachfassung werden in Änderungsantrag 178 die „data processors" und „producers" genannt.[89] Dabei handelt es sich um die Auftragsverarbeiter und Hersteller in der deutschen Sprachfassung.

III. Bewertung

Die Forderung nach einer Herstellerverantwortlichkeit taucht seit den Anfängen des Datenschutzrechts immer wieder auf. Allein diese Unnachgiebigkeit verdeutlicht, dass

[89] Englische Sprachfassung: *Albrecht*, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343en.pdf (abgerufen am 17.07.2024); deutsche Sprachfassung: *Albrecht*, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343de.pdf (abgerufen am 17.07.2024).

hier ein gewisses Defizit besteht. Während zu Zeiten der ersten deutschen Datenschutzgesetze häufig noch eine Einheit zwischen Hersteller der Soft- und Hardware und deren Verwender bestand, wird heutzutage größtenteils standardisierte Soft- und Hardware von externen Herstellern verwendet.[90] Die Verwender solcher Soft- und Hardware müssen sich dabei häufig aufgrund mangelnder Transparenz, Konfigurationsmöglichkeiten oder schlicht fehlender eigener technischer Sachkompetenz darauf verlassen, dass deren Verwendung datenschutzkonform möglich ist.[91] Ungeachtet der Möglichkeiten der Verwender trifft diese allerdings auch die Pflicht nach Art. 25 DSGVO. Dieses Missverhältnis zwischen Einfluss und Verantwortung führt regelmäßig zu Frustration bei den Verantwortlichen. Dies gilt auch dahingehend, dass ökonomische Anreize für die Hersteller aufgrund des Nachfrageverhaltens der Verwender meist nicht in dem Maße bestehen, dass es zu einer tatsächlichen Veränderung der Produkte kommt. Zudem ist zu berücksichtigen, dass Produkte oft nicht nur auf den nationalen oder den EU-Markt zugeschnitten sind. Dazu kommen in jüngerer Zeit weitere Probleme aufgrund der teilweise herstellerseitig bedingten Übermittlung von Daten in Drittländer, wie etwa die USA. Die individuellen Verwender mit Abhilfemaßnahmen und Sanktionen zu belegen, erscheint in diesem Zusammenhang bereits aus Effizienzgründen, gerade im Hinblick auf die oftmals knappen Ressourcen der Aufsichtsbehörden, kaum zweckmäßig.

Sinnvollerweise sollten hier vielmehr die Hersteller, jedenfalls im Hinblick auf technische Maßnahmen, in die Pflicht genommen werden. Damit ließe sich zum einen eine gewisse Entlastung der regulären Verantwortlichen erreichen. Zum anderen ließe sich durch eine zentrale Sanktionierung der Hersteller ein effektiveres und vor allem direkteres Anreizsystem für datenschutzkonforme Produkte etablieren. Abgesehen von Prüfpflichten oder anderen Maßnahmen seitens der Hersteller, die eine datenschutzkonforme Verwendung von entsprechender Soft- und Hardware durch die Verwender ermöglichen sollen, wäre bei standardisierten Produkten eine direkte Freistellung der Verwender für bestimmte Pflichten per Gesetz denkbar. Dies würde de facto zu einer geteilten Verantwortlichkeit für verschiedene datenschutzrechtliche Pflichten führen. Es scheint aber hinsichtlich der Folgen zweckmäßiger als etwa eine gemeinsame Verantwortlichkeit von Hersteller und Verwender anzunehmen. Alternativ könnte man Aufsichtsbehörden Abhilfemaßnahmen direkt gegen Hersteller ermöglichen.

[90] Zu denken ist insb. an Betriebssysteme wie Windows oder Mac OS, daneben auch Bürosoftware wie Office.

[91] Vgl. etwa die Probleme mit Telemetriedaten bei Windows: *Krempl*, https://www.heise.de/news/Datenschuetzer-Windows-10-Nutzer-bei-Telemetrie-nicht-aus-dem-Schneider-4976556.html (abgerufen am 17.07.2024).

Darüber hinaus sind hinsichtlich der Praktikabilität Szenarien zu bedenken, in denen eine Soft- oder Hardware zwar eine große Menge Verwender findet,[92] deren Hersteller aber nicht über datenschutzrechtliche Fachkompetenz oder Kapital für Geldbußen oder Schadensersatzansprüche verfügt, um einer Herstellerverantwortlichkeit zu begegnen.[93] Gerade im Bereich von Start-Ups und KMUs ließe sich dann über eine Einbindung von Aufsichtsbehörden in den Entwicklungsprozess und ergänzend oder alternativ eine Genehmigungspflicht der Aufsichtsbehörden für Produkte nachdenken. Ebenso denkbar wäre eine regulatorische Sandbox. Dogmatische oder systematische Argumente gegen die Begründung einer Herstellerverantwortlichkeit sind nicht ersichtlich.

H. Intermediärsverantwortlichkeit

Neben der Herstellerverantwortlichkeit wird auch eine besondere Verantwortlichkeit für Intermediäre diskutiert.[94] Auch hier handelt es sich um einen Ansatz nach noch zu schaffendem Recht. Mit Intermediären sind Stellen gemeint, die in die Kommunikation betroffener Personen eingeschaltet werden oder sonstige Leistungen für diese erbringen und dabei Daten für diese verarbeiten.[95] Dabei sollen neben Telekommunikationsdiensteanbietern und Internetprovidern auch etwa Anbieter erfasst werden, von denen bei Bedarf Programme aus dem Netz abgerufen werden können,[96] die für die betroffene Person Daten speichern oder archivieren,[97] die Dienste von Softwareagenten anbieten oder die für die betroffene Person Datenschutzfunktionen im Internet wahrnehmen („Infomediaries").[98] Diesen Beispielen sei gemein, dass die genannten Stellen nicht nur Daten über die betroffene Person im Rahmen ihres Vertragsverhältnisses (Bestandsdaten) sowie zur Erbringung der Vertragsleistung (Nutzungsdaten) verarbeiten, sondern auch weitere Daten der betroffenen Person (also Inhaltsdaten), die ihnen nur anvertraut seien. Sie sollen daher als eine Art Treuhänder fungieren. Aus dieser Stellung ergäben sich dann besondere Pflichten und besondere Risiken. Risiken sollen sich vor

[92] Etwa aufgrund kostenfreier oder kostengünstiger Nutzung beispielsweise im Start-Up-Bereich.

[93] Vgl. hierzu auch die erneute Forderung des Bundesrates im Rahmen des Evaluationsprozesses der DSGVO in BR-Drs. 639/23, S. 10 ff.

[94] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 64. Andeutungsweise a. bei: Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 121.

[95] Vgl. zum Begriff a. *Wielsch*, RW 2019, 84, 88. Zu deren Haftung im Urheberrecht: ebd., 92 f.

[96] Damit sind wohl Downloadportale gemeint.

[97] Damit könnten Anbieter von Cloud-Lösungen gemeint sein.

[98] Die etwas sperrigen Begriffe lassen sich aufgrund des Erscheinungsjahres 2001 erklären.

allem aus dem Zugriff des Intermediäres auf die Daten der betroffenen Person und damit die Verarbeitung für dessen eigene Zwecke, aber auch aufgrund der leichteren Kenntnisnahme durch Dritte beim Intermediär ergeben.

Im Rahmen der Empfehlungen des BMI-Gutachtens zur „Modernisierung des Datenschutzrechts" (2001) wurde allerdings noch keine eigene Regelung der Intermediäre im Datenschutzrecht angeregt, da diese als Verantwortliche bereits datenschutzrechtlich reguliert wären.[99] Spezifische gesetzliche Vorgaben für Intermediäre seien nicht erforderlich. Weitergehende Regeln sollten dem vertraglichen Verhältnis zwischen Intermediär und betroffener Person überlassen werden. Generell solle aber die weitere Entwicklung von Intermediären beobachtet werden. Insofern könne langfristig eine eigenständige Regelung erforderlich sein.

Ob eine dedizierte Regelung von Intermediären dazu beiträgt, die Defizite des Konzeptes der Verantwortlichkeit zu kompensieren oder zu beheben, ist eher zweifelhaft.[100] So stellt *Roßnagel* in seinem 2019 erschienen Gutachten zur „Evaluation der DSGVO aus Verbrauchersicht" fest, dass etwa hinsichtlich von Social Networks eine Unterscheidung zwischen Hersteller und Anwender weitgehend bedeutungslos sei, da der Verantwortliche entweder Hersteller sei oder jedenfalls einen so starken Einfluss auf Hersteller habe, dass er sie zwingen könne das von ihm gewünschte Maß an Datenschutz zu realisieren.[101] Schwierigkeiten bereitet bei der Analyse der Verantwortlichkeit von Intermediären nicht die Verantwortlichkeit des Intermediärs als Anbieter, sondern vielmehr das Verhältnis zwischen Infrastrukturnutzern und Anbietern im Hinblick auf die Verantwortlichkeit der Infrastrukturnutzer. So stellt sich regelmäßig die Frage, ob ein Intermediär auch für Handlungen des Nutzers verantwortlich ist. Deutlich wird diese Verantwortlichkeit für fremde Inhalte etwa im Urteil des EuGH in der Rechtssache Google Spain und die eigene Verantwortlichkeit der Suchmaschine für die Inhalte der aufgelisteten Webseiten.[102] Umgekehrt zeigt sich in den Urteilen des EuGH in den Rechtssachen Wirtschaftsakademie und Fashion ID die Frage,[103] inwiefern ein Nutzer fremder Infrastruktur für Verarbeitungen durch diese verantwortlich ist. Insofern lässt sich die Problematik hinsichtlich von Intermediären auch weniger als Verantwortlichkeitsdefizit begreifen, sondern vielmehr als Frage welche Anforderungen der DSGVO für Intermediäre sinnvoll sind und welche gegebenenfalls noch fehlen.

---

[99] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 64.

[100] Kritisch etwa: *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 328 ff.

[101] *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 51.

[102] EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857.

[103] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

Auch wenn der Fokus bei Intermediären häufig auf sozialen Netzwerken und Plattformen[104] liegt, dürfen dabei auch klassische Cloud-Anbieter, Host-Provider und sonstige Infrastrukturanbieter, wie etwa Analyse-Anbieter, nicht vergessen werden. Maßgeblich ist hier vor allem die Frage, wie eine sinnvolle Abgrenzung zwischen Auftragsverarbeiter und gemeinsam Verantwortlichen erfolgen kann. Zielführender als eine gesonderte Reglung von Intermediären wäre es daher, die Voraussetzungen einer gemeinsamen Verantwortlichkeit zu präzisieren. Weiterhin könnte man eine Anwendung der Privilegierungen aus dem DSA auf bestimmte Intermediäre erwägen.[105] Dies würde den Wertungswiderspruch zwischen datenschutzrechtlicher Verantwortlichkeit und zivil- und strafrechtlicher Haftung entschärfen.[106] Darüber hinaus stellt sich insbesondere im Hinblick auf private Nutzer die Frage, ob die DSGVO überhaupt anwendbar ist.[107] Isoliert scheint eine Regelung der Intermediäre, auch im Hinblick darauf wie diese konkret zu definieren wären, bislang nicht zielführend.

Inwiefern die Regelungen des DSA und gegebenenfalls auch des DMA indirekt die datenschutzrechtlichen Besonderheiten von Intermediären erfassen können, bleibt abzuwarten, auch weil die meisten dieser Regelungen spezifische Kontexte betreffen wie etwa Werbung auf Online-Plattformen (Art. 26 DSA).

I. Haushaltsausnahme

Ein weiterer Ansatz, insbesondere um einer zu weiten Anwendung der gemeinsamen Verantwortlichkeit entgegenzuwirken, könnte ein breiteres Verständnis der sogenannten Haushaltsausnahme aus Art. 2 Abs. 2 lit. c DSGVO sein. Zwar erfasst die Haushaltsausnahme nur eine bestimmte Kategorie von Akteuren, nämlich natürliche Personen, allerdings könnten hiermit zahlreiche Verarbeitungsszenarien abgedeckt werden. Im Gegensatz zu den bislang vorgeschlagenen Ansätzen würden bei einem breiteren Verständnis der Haushaltsausnahme nicht weitere Arten der Verantwortlichkeit geschaffen oder modifiziert, sondern die Verarbeitung in einem bestimmten Kontext von vorneherein aus der Anwendung der DSGVO ausgeschlossen werden. Damit würden die betroffenen Personen auch nicht als (gemeinsame) Verantwortliche gelten. Dies

[104] Zu einer dedizierten Plattform-Verantwortlichkeit: *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 316 ff.

[105] Dazu: Kapitel 5 D. Anwendung der DSA-Privilegierungen.

[106] Vgl. BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, Rn. 35.

[107] Dazu: Kapitel 5 I. Haushaltsausnahme.

könnte zu einer klareren Verantwortlichkeitsverteilung beitragen. Da die Anwendbarkeit der Haushaltsausnahme bislang maßgeblich von der Rechtsprechung des EuGH abhängt, wäre ein breiteres Verständnis rechtssicher nur de lege ferenda denkbar.

I. Gesetzeslage

Soweit die sogenannte Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO Anwendung findet, ist die DSGVO trotz der Verarbeitung personenbezogener Daten nicht anwendbar. Soweit die DSGVO insgesamt nicht anwendbar ist, besteht dann im Anwendungsbereich der Haushaltsausnahme auch keine Verantwortlichkeit. Voraussetzung für die Anwendung der Haushaltsausnahme ist eine Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.[108] Gem. ErwGr 18 S. 1 DSGVO darf bei einer solchen Verarbeitung i.S.v. Art. 2 Abs. 2 lit. c DSGVO kein Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit bestehen.[109] Nach ErwGr 18 S. 3 DSGVO soll die DSGVO für Verantwortliche oder Auftragsverarbeiter, die die Instrumente[110] für die Verarbeitung für solche persönlichen oder familiären Tätigkeiten bereitstellen nichtsdestotrotz aber weiterhin gelten.[111] Damit gilt die Haushaltsausnahme etwa für Personen, die privat[112] innerhalb einer Familie Fotos über einen Cloud-Dienst teilen. Für den Anbieter dieses Clouddienstes gilt die Haushaltsausnahme aber wiederum nicht. In Verarbeitungsszenarien mit gemeinsam Verantwortlichen gilt die Haushaltsausnahme, entsprechend ihrem Wortlaut, nur für den gemeinsam Verantwortlichen, dessen Verarbeitung in einem persönlichen oder familiären Kontext stattfindet.[113] Was sich der Unionsgesetzgeber unter ausschließlich persönlich oder familiären Tätigkeiten vorstellt, wird in ErwGr 18 S. 2 DSGVO näher erläutert: „[...] das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten [...]". ErwGr 18 S. 2 DSGVO („könnte") ist vorsichtiger formuliert als dessen DSRL-Entsprechung ErwGr 12 S. 2 DSRL („auszunehmen ist"). Dies dürfte

[108] Zu den Elementen „persönlich" und „familiär": Simitis/Hornung/Spiecker/*Roßnagel*, Art. 2 DSGVO, Rn. 24 f.

[109] Vgl. Kühling/Buchner/*Kühling/Raab*, Art. 2 DS-GVO, Rn. 26. Ausführlich: G/S/S/V/*Grafenstein*, Art. 2 DSGVO, Rn. 36 ff.

[110] Diese werden im Folgenden mit „(fremder) Infrastruktur" gleichgesetzt.

[111] Insofern ist hier a. eine Annahme der fehlenden Verantwortlichkeit vergleichbar zu ErwGr 47 DSRL explizit ausgeschlossen. Vgl. a. *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 29.

[112] Nicht aber öffentlich.

[113] So a.: *Wagner*, ZD 2018, 307, 311 Fn. 50.

im Zusammenhang mit dem relativ strengen Urteil des EuGH in der Rechtssache Lindqvist[114] einerseits und der Erwähnung der Nutzung sozialer Netze in ErwGr 18 S. 2 DSGVO andererseits stehen.[115] Die Vermutung liegt daher nahe, dass man im Gesetzgebungsprozess zur DSGVO Reformbedarf im Hinblick auf die Haushaltsausnahme erkannt hatte, sich aber nicht auf eine konsequente Umsetzung einigen konnte.[116]

II. Rechtsprechung des EuGH

Aufgrund der Diskrepanzen zwischen ErwGr 18 S. 2 DSGVO und der bisherigen Rechtsprechung des EuGH ist die Verantwortlichkeit von privaten Nutzern daher bislang unklar, wenn diese fremde oder geteilte Infrastruktur verwenden, also etwa bei der Verwendung von Social Media, IoT-Geräten, Smart Cars, Smart Homes u.ä., soweit dort personenbezogene Daten verarbeitet werden. Zwar hatte der EuGH im Urteil in der Rechtssache Wirtschaftsakademie[117] für soziale Netzwerke festgehalten, dass der bloße Umstand der Nutzung[118] keine Mitverantwortlichkeit für die Nutzer der Plattform begründe.[119] Er hatte allerdings nicht weiter ausgeführt, woraus sich diese fehlende Verantwortlichkeit ergibt. Der EuGH hatte sich also auch nicht explizit auf die Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO berufen.[120] Gerade im Hinblick auf soziale Netzwerke drängt sich unabhängig von der Begründung daneben auch die Frage auf, wie der Begriff der Nutzung zu verstehen ist. Inwiefern wären hiervon etwa ein eigenes Profil, eigene Posts, die Verlinkungen von anderen Nutzern, der Upload von Fotos und Videos oder ähnliches erfasst? Auch hierzu finden sich keine weiteren Ausführungen des EuGH. Ausgehend von den Urteilen in den Rechtssachen Wirtschaftsakademie und Fashion ID[121], scheint ein kommerzielles oder jedenfalls nicht mehr genuin privates Interesse an der Nutzung eines sozialen Netzwerks ein mögliches Differenzierungskriterium zwischen einer Nutzung als unbeachtlicher „bloßer Nutzer“

[114] EuGH, Urteil vom 06.11.2003 – C-101/01 (Lindqvist) = EuGRZ 2003, 714-722.

[115] Dazu unten.

[116] Vgl. Kuner/Bygrave/Docksey/*Kranenborg*, Art. 2 GDPR, 68; Ehmann/Selmayr/*Zerdick*, Art. 2 DS-GVO, Rn. 11. Kritisch: *Art. 29-Datenschutzgruppe*, Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 27.02.2013.

[117] Dazu: Kapitel 4 B. I. Wirtschaftsakademie.

[118] Allein der Begriff der Nutzung scheint hier nicht eindeutig. So können etwa nach Art. 2 lit. d e-Commerce-RL Nutzer auch Informationen zugänglich machen und nicht nur abfragen. Vgl. a.: ErwGr 20 e-Commerce-RL.

[119] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 35.

[120] Kuner/Bygrave/Docksey/*Bygrave/Tosoni*, Art. 4 (7) GDPR, 154 gehen davon aus, dass der Nutzer sich nicht selbst gegenüber Verantwortlicher sein könne.

[121] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

und einer Nutzung als gemeinsam Verantwortlicher zu sein.[122] So handelte es sich in dem einen Sachverhalt um den Bildungsdienstleister einer IHK und im anderen Sachverhalt um ein Modekaufhaus. Unabhängig vom Kontext der Verarbeitung bildete in der Rechtssache Wirtschaftsakademie eine Facebook (Fan-)Page aber auch rein technisch eine separate Kategorie gegenüber den regulären Nutzerprofilen.[123]

Geht man davon aus, dass sich der EuGH mit dem „bloßen Umstand der Nutzung" auf die Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO bezogen hat, stellen sich allerdings Folgeprobleme. So ist gerade bei Sachverhalten im Internet die Anwendung der Haushaltsausnahme grundsätzlich im Konflikt mit dem Urteil des EuGH in der Rechtssache Lindqvist. In der Rechtssache Lindqvist hatte der EuGH geurteilt, dass die Veröffentlichung personenbezogener Daten, die einer unbegrenzten Zahl von Personen zugänglich sei, die Anwendbarkeit der Haushaltsausnahme ausschließe.[124] Problematisch erscheint neben der Rechtssache Lindqvist auch das Urteil des EuGH in der Rechtssache Rynes, wonach die Haushaltsausnahme nicht greifen soll, sobald die Verarbeitung sich auch auf den öffentlichen Raum, also einen Bereich außerhalb der privaten Sphäre, erstrecke.[125] In Jehovan todistajat[126] hatte der EuGH die Rechtsprechung in den Rechtssachen Lindqvist und Rynes noch einmal bestätigt.[127] Man kann also aufgrund der Rechtsprechung des EuGH von einer Beschränkung der Haushaltsausnahme in quantitativer wie qualitativer Hinsicht sprechen.[128] Daneben legt der EuGH Ausnahmen von der Anwendbarkeit des Datenschutzrechts, wie eben auch die Haushaltsausnahme, grundsätzlich eng aus.[129]

---

[122] Vgl. a. *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, 6.

[123] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 2 f.

[124] EuGH, Urteil vom 06.11.2003 – C-101/01 (Lindqvist) = EuGRZ 2003, 714-722, Rn. 47; EuGH, Urteil vom 16.12.2008 – C-73/07 (Satamedia) = MMR 2009, 175, Rn. 43 f.; zuletzt: EuGH, Urteil vom 14.02.2019 – C-345/17 (Buivids) = ZD 2019, 262, Rn. 37 ff.

[125] EuGH, Urteil vom 11.12.2014 – C-212/13 (Rynes) = ZD 2015, 77, Rn. 33.

[126] Dazu: Kapitel 4 B. II. Jehovan todistajat.

[127] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 42. Vgl. a. *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 28.

[128] *Golland*, ZD 2020, 397, 397; vgl. Kühling/Buchner/*Kühling/Raab*, Art. 2 DS-GVO, Rn. 24 f.; BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, Rn. 15. *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 19 f., 90 f. fordert eine ausdifferenzierte Regelung de lege ferenda.

[129] Zuletzt: EuGH, Urteil vom 09.07.2020 – C-272/19 (VQ/Hessen) = NVwZ 2020, 1497, Rn. 68; ebenso: EuGH, Urteil vom 04.05.2017 – C-13/16 (Rigas) = DAR 2017, 698, Rn. 30; vgl. für die DSRL Dammann/Simitis DSRL/*Simitis*, Einleitung, Rn. 22 f.

III. Position der Aufsichtsbehörden

Die Art. 29-Datenschutzgruppe hielt in WP 163 (zur Nutzung sozialer Online-Netzwerke) fest, dass die Nutzer sozialer Netzwerke üblicherweise nicht Verantwortliche, sondern betroffene Personen seien.[130] Soweit die Nutzer nicht nur betroffene Personen seien, sollten sie aber grundsätzlich der Haushaltsausnahme unterfallen. Die Haushaltsausnahme gelte dann nicht mehr, wenn Nutzer das soziale Netzwerk für die Zusammenarbeit eines Verbandes, einer Gesellschaft oder eines Unternehmens nutzen würden. Ebenso solle die Haushaltsausnahme dann nicht gelten, wenn Nutzer das soziale Netzwerk hauptsächlich zur Förderung kommerzieller, politischer oder karitativer Zielsetzungen nutzen würden. Daneben könne eine hohe Anzahl von Kontakten eines Nutzers gegen eine Anwendung der Haushaltsausnahme sprechen.[131] In Einklang mit der Rechtsprechung in der Rechtssache Lindqvist solle zudem ein im sozialen Netzwerk öffentlich zugängliches Profil oder die externe Indexierung des Profils durch Suchmaschinen die Haushaltsausnahme aushebeln. Schließlich gelte die Haushaltsausnahme dann nicht mehr, wenn der Nutzer sich bewusst entscheide die Zugriffsmöglichkeit auf seine Inhalte über den Kreis seiner Kontakte hinaus auszudehnen.[132] Neben der Haushaltsausnahme wies die Art. 29-Datenschutzgruppe noch auf andere Ausnahmeregelungen, wie die Verarbeitung zu journalistischen, künstlerischen oder literarischen Zwecken, hin.[133] Festhalten lässt sich, dass das WP 163 grundsätzlich der Rechtsprechung des EuGH folgte.

Dieses Verständnis aus WP 163 findet sich auch im Beispiel 12 in dem späteren WP 169 der Art. 29-Datenschutzgruppe.[134] Dort wurden soziale Netzwerke als Online-Kommunikationsplattformen verstanden, über die Einzelpersonen Informationen veröffentlichen und mit anderen Nutzern austauschen können. Die Anbieter sozialer Netzwerke sollen dabei Verantwortliche für die von den Einzelpersonen veröffentlich-

---

[130] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, 6.

[131] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, 7; ähnlich: *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 28. A. die reine Deklaration als „Freund" dürfte kaum Wert haben: *Golland*, ZD 2020, 397, 398.

[132] Vgl. a. *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 28.

[133] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, 7.

[134] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 26.

ten Informationen sein, da sie sowohl über die Zwecke wie auch die Mittel der Verarbeitung dieser Informationen entscheiden. Die Nutzer solcher Netzwerke wiederum seien dann als Verantwortliche einzustufen, wenn sie personenbezogene Daten Dritter hochladen würden, sofern sie nicht unter die Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO fielen. Für den Fall, dass ein Nutzer nicht unter die Haushaltsausnahme fiele, wäre dann wohl von einer gemeinsamen Verantwortlichkeit des Nutzers und des Anbieters hinsichtlich der Inhaltsdaten des Nutzers auszugehen, denn es liegen gemeinsame Mittel[135] vor. Zu einer solchen gemeinsamen Verantwortlichkeit verhält sich die Art. 29-Datenschutzgruppe allerdings nicht.

IV. Modernisiertes Übereinkommen Nr. 108 des Europarates

Ausführungen zu der Haushaltsausnahme finden sich auch im „Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (CETS 223).[136] Zwar ist das Übereinkommen Nr. 108 des Europarates ein von der DSGVO unabhängiges Vertragswerk, aufgrund der starken Wechselwirkung zwischen Übereinkommen Nr. 108 und der DSRL einerseits sowie der DSGVO und dem modernisierten Übereinkommen Nr. 108 anderseits[137] dürften, auch im Hinblick auf Art. 8 EMRK, die Erwägungen des Europarates aber hilfreich sein. Nach diesem Explanatory Report sollen durch die Haushaltsausnahme aufgrund eines Bezugs zu Aktivitäten im Privatleben unverhältnismäßige Pflichten für eine Verarbeitung in der privaten Sphäre eines Individuums ausgeschlossen werden.[138] Aktivitäten im persönlichen und familiären Bereich seien eng und objektiv mit dem Privatleben eines Individuums verknüpft und würden die Privatsphären anderer Menschen nicht außergewöhnlich berühren. Diese Aktivitäten hätten auch keine professionellen oder kommerziellen Aspekte. Das Teilen von Daten innerhalb der privaten Sphäre soll als Teilen innerhalb einer Familie, eines beschränkten Kreises von Freunden oder eines Kreises der größenmäßig beschränkt sei und auf persönlichen Verhältnissen oder einem besonderen Vertrauensverhältnis basiere verstanden werden.

[135] Zu den Zwecken siehe unten.

[136] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018.

[137] So wird das modernisierte Übereinkommen Nr. 108 des Europarates auch als „GDPR-lite" bezeichnet.

[138] *Council of Europe*, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 18.05.2018, Rn. 27.

V. Kriterien für die Anwendung

Interessant ist die Anwendung der Haushaltsausnahme vor allem im Hinblick auf soziale Netze sowie Online-Tätigkeiten, da sich hier gegenüber der DSRL aus dem Jahr 1995 ein deutlich höherer Anwendungsbereich ergibt. Die Erwähnung der „[...] Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten[139] [...]" in ErwGr 18 S. 2 DSGVO, verbunden mit dem Hinweis auf die Anwendbarkeit der DSGVO für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für eine solche Verarbeitung bereitstellen, ist auch die wesentliche Neuerung der DSGVO gegenüber der DSRL. Die Nutzung sozialer Netze im Sinne des ErwGr 18 S. 2 DSGVO wird dabei häufig so verstanden, dass sie nur dann entsprechend privilegiert sei, wenn die Verarbeitung nur innerhalb der beschränkten „Öffentlichkeit" einer Gruppe oder ausgewählter Personen erfolge.[140] Das reine Registrierungserfordernis eines sozialen Netzes sei für diese beschränkte Öffentlichkeit nicht ausreichend.[141] Unerheblich sei auch die subjektive Vorstellung des Nutzers über den Adressatenkreis der Veröffentlichung.[142] Würden tatsächlich weitere, nicht intendierte Adressaten durch die Veröffentlichung erreicht, erlösche damit die Privilegierung durch die Haushaltsausnahme. Ebenso sei für die Anwendbarkeit der Haushaltsausnahme nicht das Objekt oder der Ort der Verarbeitung (etwa die Cloud) maßgeblich, sondern allein der Kontext der Verarbeitung.[143] Einheitliche Vorgaben für den Umfang an Öffentlichkeit, der noch unter die Haushaltsausnahme falle, ließen sich kaum allgemein bilden und dürften vielmehr je nach Kontext variieren.[144]

Jenseits der Zugänglichkeit personenbezogener Daten gegenüber einer unbegrenzten Anzahl von Personen ist daher bislang unklar, wann eine quantitative Grenze der Haushaltsausnahme erreicht ist.[145] Insbesondere bei sozialen Netzen dürfte ab einer gewissen Anzahl von „Kontakten" oder „Freunden" keine persönliche Tätigkeit oder Beziehung mehr vorliegen. Jedenfalls im Hinblick auf den Anbieter der Infrastruktur liegt

---

[139] Also des Führens eines Schriftverkehrs oder von Anschriftenverzeichnissen.

[140] Kühling/Buchner/*Kühling/Raab*, Art. 2 DS-GVO, Rn. 25; *Golland*, ZD 2020, 397, 398 m.w.N. BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, Rn. 19 erwägt ein Beherrschbarkeitskriterium zu berücksichtigen. Paal/Pauly/*Ernst*, Art. 2 DSGVO, Rn. 21 hingegen will die Anwendbarkeit der Haushaltsausnahme bereits ausschließen, sofern sich ein Diensteanbieter Rechte an den Daten vertraglich zusichert.

[141] *Golland*, ZD 2020, 397, 398.

[142] *Golland*, ZD 2020, 397, 398.

[143] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 41; *Golland*, ZD 2020, 397, 398.

[144] *Golland*, ZD 2020, 397, 398.

[145] *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 20.

aber keine persönliche Beziehung vor. Die Beziehung zum Anbieter der Infrastruktur muss aber nach ErwGr 18 S. 2 DSGVO unbeachtlich bleiben. Daneben kann man in qualitativer Hinsicht hinterfragen, inwiefern je nach Verarbeitungskontext personenbezogene Daten veröffentlicht oder eher übermittelt werden. Ohne eine Klarstellung des EuGH scheint jedenfalls die aktive Nutzung sozialer Netzwerke in Form von Posts, dem Erstellen von Verlinkungen und dem Upload von Videos und Fotos nach wie vor problematisch. Daher kann man ErwGr 18 S. 2 DSGVO auch als Aufforderung des Unionsgesetzgebers an den EuGH zu einem Überdenken seiner Rechtsprechung verstehen. Abseits des Kriteriums der Öffentlichkeit einer Verarbeitung ist auch das Kriterium des öffentlichen Raums problematisch bei Dashcams, Drohnen und Wearables u.Ä.[146] Diese Unklarheiten sind äußerst bedauerlich, denn die Frage der Anwendbarkeit der Haushaltsausnahme ist im Hinblick auf ihre Folgen keinesfalls trivial. Sofern die Haushaltsausnahme nicht anwendbar ist, trifft den Nutzer einer fremden Infrastruktur, wie einem sozialen Netz, nämlich die Verantwortlichkeit mit allen ihren Pflichten und Konsequenzen.[147]

Teilweise wird im Hinblick auf ErwGr 18 S. 2 DSGVO und die bisherige EuGH-Rechtsprechung daher zumindest eine Teilrevision des Urteils in der Rechtssache Lindqvist gefordert.[148] Die Haushaltsausnahme wird demnach so verstanden, dass die Nutzung sozialer Netze durch Privatpersonen generell, unabhängig von Einschränkungen des Adressatenkreises, der Haushaltsausnahme unterfalle.[149] Als Argument hierfür wird angeführt, dass Posts in sozialen Netzen selten eine nennenswerte Breitenwirkung entfalten würden und dass eine differenzierte Anwendung der Haushaltsausnahme nicht praktikabel wäre.[150] Eine Rechtssicherheit sei hinsichtlich der Haushaltsausnahme kaum gegeben und die technische Entwicklung ohnehin dynamisch. Hinsichtlich dieser Annahmen lässt sich bereits hinterfragen, inwiefern etwa bei Diensten wie Twitter keine Breitenwirkung bestünde. Das dargestellte Verständnis dürfte zwar sicherlich die Anwendbarkeit der Haushaltsausnahme erleichtern, allerdings ist fraglich, wie es mit dem Wortlaut und Telos der Norm zu vereinbaren wäre.[151] Denn zunächst

[146] *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 20.

[147] *Wagner*, ZD 2018, 307, 308; warnend: *Golland*, ZD 2020, 397, 399.

[148] BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, Rn. 21.

[149] Vermittelnd: G/S/S/V/*Grafenstein*, Art. 2 DSGVO, Rn. 46 ff.

[150] BeckOK DatenschutzR[47]/*Bäcker*, Art. 2 DSGVO, 20 f.

[151] Berechtigt ist insofern die Kritik von *Golland*, ZD 2020, 397, 398, dass bei einer generellen Anwendung der Haushaltsausnahme die Rechtsprechung aus EuGH, Urteil vom 06.11.2003 – C-101/01 (Lindqvist) = EuGRZ 2003, 714-722 ignoriert würde.

einmal spricht Art. 2 Abs. 2 lit. c DSGVO von der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Sofern man persönliche und familiäre Tätigkeiten als Verarbeitungen mit einem ähnlichen Umfang betroffener Personen versteht, dürfte die Nutzung eines sozialen Netzes im Rahmen eines Posts mit unbegrenzter Öffentlichkeit hier nicht mehr darunterfallen. ErwGr 18 S. 2 DSGVO führt als weitere Beispiele für Tätigkeiten das Führen von Schriftverkehr oder von Anschriftenverzeichnissen an. Das Führen von Schriftverkehr als Kommunikationshandlung besteht aber regelmäßig mit einer überschaubaren Anzahl von Beteiligten und ein Anschriftenverzeichnis dient der Vorbereitung von Kommunikation. Das Veröffentlichen eines Posts in sozialen Netzwerken ist demgegenüber eine klassische one-to-many-Kommunikation. Denkbar erscheint es daher eher, die Möglichkeit von Nachrichten zwischen Nutzern eines sozialen Netzes unter die Haushaltsausnahme zu fassen als deren öffentliche Posts. Aufgrund der Begriffe „persönlich" und „familiär" liegt zudem ein Verständnis im Sinne des Art. 7 GRCh nahe. Versteht man die Haushaltsausnahme als Auflösung eines grundrechtlichen Konfliktes zwischen dem Recht auf Achtung des Privat- und Familienlebens gem. Art. 7 GRCh und dem Recht auf den Schutz personenbezogener Daten gem. Art. 8 GRCh zugunsten von Art. 7 GRCh,[152] dürfte diese Ausnahme im Rahmen praktischer Konkordanz eng zu verstehen sein. Auch dies spricht gegen eine Anwendung der Haushaltsausnahme auf soziale Netze insgesamt. Will man die Anwendung der Haushaltsausnahme dennoch auf die Nutzung sozialer Netze insgesamt erstrecken, dürfte hierfür eine reine Änderung der Rechtsprechung des EuGH also nicht mehr ausreichen bzw. möglich sein. Zu fordern wäre vielmehr eine entsprechende Änderung von Art. 2 Abs. 2 lit. c DSGVO selbst. Aufgrund dieses Anwendungsdilemmas sieht sich die enge Auslegung der Haushaltsausnahme insgesamt wachsender Kritik ausgesetzt.[153] Dies gilt insbesondere für Verarbeitungen, die sowohl im Rahmen von privaten wie beruflichen Tätigkeiten erfolgen.[154] Teilweise wird dort ein Abstellen auf den Schwerpunkt der Tätigkeit gefordert.

VI. Konsequenzen für die Verantwortlichkeit

Welche Konsequenzen hat nun die Haushaltsausnahme für die Verantwortlichkeit? Zwar hebelt die Haushaltsausnahme in Art. 2 Abs. 2 lit. c DSGVO die Anwendung der

[152] Vgl. *Heberlein*, DVBl[135] (2020), 1225, 1228.

[153] Kühling/Buchner/*Kühling/Raab*, Art. 2 DS-GVO, Rn. 28; *Golland*, ZD 2020, 397, 397 m.w.N. Für eine noch restriktivere Auslegung hingegen: *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, 26.11.2019, 20 ff.

[154] *Wagner*, ZD 2018, 307, 311 mit Beispielen.

DSGVO nur aufgrund des Kontextes einer Verarbeitung aus, also nicht aufgrund einer bestimmten Einordnung eines Verantwortlichen. Sofern die DSGVO aber nicht anwendbar ist, entfällt auch eine damit verbundene Verantwortlichkeit, im Falle der Haushaltsausnahme von natürlichen Personen. Wie bei der Verantwortlichkeit allgemein ist auch bei der Anwendung der Haushaltsausnahme zunächst maßgeblich, für welche Verarbeitungsvorgänge die Verantwortlichkeit einer natürlichen Person theoretisch bestehen könnte, um davon ausgehend deren Anwendbarkeit zu prüfen.[155] Gerade im Hinblick auf die Nutzung fremder Infrastruktur, wie etwa soziale Netze, und eine potenzielle gemeinsame Verantwortlichkeit muss daher eine Analyse der jeweiligen Entscheidungsbeiträge zu den Zwecken und Mitteln der Verarbeitungsvorgänge erfolgen.[156]

Die folgende Darstellung beschäftigt sich aus Anlass von ErwGr 18 S. 2 DSGVO mit der Haushaltsausnahme bei der Verwendung fremder Infrastruktur, insbesondere bei sozialen Netzen. Grundsätzlich lässt sich bei der Nutzung fremder Infrastrukturen eine Unterscheidung zwischen Inhaltsdaten und Nutzungsdaten treffen.[157] Inhaltsdaten werden durch den Nutzer der Infrastruktur erzeugt. Nutzungsdaten über die Nutzer werden von dem Anbieter im Hintergrund erfasst.[158] Bei der Analyse der maßgeblichen Verarbeitungsvorgänge muss daher auch berücksichtigt werden, ob es sich um eine Verarbeitung von Inhalts- oder Nutzungsdaten handelt. Die Verantwortlichkeit der Nutzer kann sich sowohl auf die Inhalts- wie auch die Nutzungsdaten beziehen, die im Rahmen der intendierten Nutzung einer fremden Infrastruktur, wie etwa bei einem Post in einem sozialen Netz, anfallen. Unerheblich sind hingegen die Daten des Nutzers, die sich auf ihn selbst beziehen, maßgeblich sind vielmehr die Daten Dritter.[159] So können in einem Post im Rahmen von Inhaltsdaten Dritte erwähnt oder verlinkt werden oder durch den Besuch des Profils eines Nutzers entsprechende Nutzungsdaten von Dritten seitens des Anbieters erfasst werden.[160]

[155] Vgl. *Golland*, ZD 2020, 397, 399.
[156] Vgl. *Wagner*, ZD 2018, 307, 308.
[157] So a.: *Wagner*, ZD 2018, 307, 309; ähnlich: *Golland*, ZD 2020, 397, 399.
[158] Also etwa Cookies, Verlauf, Fingerprinting etc.
[159] Vgl. *Golland*, ZD 2020, 397, 398 f.; Simitis/Hornung/Spiecker/*Roßnagel*, Art. 2 DSGVO, Rn. 18.
[160] *Wagner*, ZD 2018, 307, 309 mit weiteren Beispielen. Allerdings dürfte eine Fanpage nach der Rechtssache Wirtschaftsakademie, aber a. bereits im Hinblick auf *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, 6, eindeutig nicht unter die Haushaltsausnahme fallen.

1. Haushaltsausnahme und (gem-)einsame Verantwortlichkeit

Regelmäßig wird ein Nutzer mit der Verarbeitung von Inhaltsdaten seine eigenen Zwecke verfolgen, der Anbieter der Infrastruktur mit der Verarbeitung von Nutzungsdaten wiederum andere eigene Zwecke verfolgen. Dabei wissen Nutzer und Anbieter allerdings, dass die Möglichkeit der Nutzung der Infrastruktur zur Verarbeitung der Inhaltsdaten gerade bei einem kostenfreien Angebot nur durch die Inkaufnahme der Verarbeitung der Nutzungsdaten stattfinden kann.[161] Finden sich die Zwecke von Nutzer und Anbieter in solch einem wechselseitigen Billigungsverhältnis,[162] kann aufgrund des Entscheidungsbeitrags des Nutzers, also der Ermöglichung der Verarbeitung der Nutzungsdaten Dritter,[163] sowie der anderweitigen Entscheidungsbeiträge des Anbieters bezüglich der Mittel,[164] eine gemeinsame Verantwortlichkeit bestehen.[165] Denn gemeinsame Mittel bestehen somit unproblematisch. Diese theoretische gemeinsame Verantwortlichkeit bezieht sich dann sowohl auf die Inhalts- wie auch die Nutzungsdaten. Die gemeinsame Verantwortlichkeit des Nutzers in Bezug auf die Nutzungsdaten würde allerdings nur für deren Erhebung durch den Anbieter gelten.[166] Liegen nun die Voraussetzungen der Haushaltsausnahme vor, würde nach Maßgabe des ErwGr 18 S. 3 DSGVO die Verantwortlichkeit des Nutzers entfallen, während die des Anbieters bestehen bliebe.[167]

Kehrseite dieses wechselseitigen Billigungsverhältnisses wäre für den Anbieter wie dargestellt, dass dieser für die Verarbeitung der Inhaltsdaten des Nutzers gemeinsam verantwortlich wäre.[168] Denkbar ist hinsichtlich der gemeinsamen Mittel vor allem ein Einfluss des Anbieters auf die Arten von personenbezogenen Daten oder die Kategorien von betroffenen Personen im Sinne von Art. 28 Abs. 3 DSGVO. Somit würde der Anbieter Entscheidungen über wesentliche Elemente der Mittel treffen. So dürfte er

[161] A. der umgekehrte Fall ist im Rahmen von Analyseangeboten denkbar.

[162] Zu denken wäre hier an die Rechtssachen Wirtschaftsakademie oder Fashion ID, dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[163] Insofern also zu pauschal im Hinblick auf die Mittel, dann wiederum widersprüchlich im Hinblick auf eine conditio sine qua non: *Wagner*, ZD 2018, 307, 309.

[164] Dazu unten.

[165] Etwas ähnliches meint wohl *Wagner*, ZD 2018, 307, 309 mit den sich gegenseitig bedingenden Einwirkungssphären. Ablehnend: *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 8.

[166] Vgl. zur Erhebung und Übermittlung EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, 76.

[167] Vgl. hierzu a. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 164 ff.

[168] Vgl. EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 73. A. ErwGr 18 DSGVO differenziert nicht zwischen Inhalts- und Nutzungsdaten. Ebenso dürfte ErwGr 47 DSRL nicht analog anwendbar sein, vgl. *Brühann*, DuD[28] (2004), 201, 205.

regelmäßig die Entscheidung darüber treffen, wann Daten gelöscht werden und potenziell auch, ob Dritte Zugriff auf diese Daten haben.[169] Insbesondere die Anzeige der Inhaltsdaten (welche) gegenüber anderen Nutzern (wem) und in welcher Priorität (wo) in einem sozialen Netz unterliegt der Entscheidung durch den Anbieter.[170] Zudem kann bei sozialen Netzen eine Moderation[171] erfolgen oder können allgemein bei Anbietern von Infrastruktur automatisierte oder manuelle Prüfsysteme vorhanden sein, die die Inhalte der Nutzer untersuchen. Ein Entscheidungsbeitrag kann sich ebenso aus redaktionellen Vorgaben ergeben, etwa ob ein Freitextfeld vorliegt, eine Auswahl besteht oder ähnliches.[172] Jedenfalls liefert der Anbieter Entscheidungsbeiträge hinsichtlich der technischen und organisatorischen Maßnahmen der Verarbeitung der Inhaltsdaten.[173] Daneben sind auch Entscheidungsbeiträge zu den Zwecken einer Verarbeitung über thematische Sparten oder Kategorien denkbar.[174]

Zwar soll nach Ansicht der Art. 29-Datenschutzgruppe eine Verantwortlichkeit erst dann bestehen, wenn ein Akteur über wesentliche Elemente der Mittel entscheidet,[175] dies kann allerdings nur soweit gelten, wie überhaupt ein Auftragsverarbeiter beteiligt ist.[176] Ist kein Auftragsverarbeiter beteiligt, wäre der Akteur, der nur über technische und organisatorische Maßnahmen entscheidet, sonst ein datenschutzrechtliches Nullum.[177] Da die Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO nicht zwischen wesentlichen und unwesentlichen Elementen der Mittel unterscheidet, ist eine Entscheidung über die wesentlichen Elemente der Mittel bereits vom Wortlaut her nicht notwendig für eine gemeinsame Verantwortlichkeit in diesem Szenario. Grundsätzlich denkbar wäre zwar auch eine Auftragsverarbeitung hinsichtlich der Inhaltsdaten durch den Anbieter, diese wird aber regelmäßig an der fehlenden Weisungsgebundenheit des Anbieters scheitern.[178] Teleologisch wäre es aufgrund des weiten Verständnisses des

[169] Zu denken wäre etwa an Fälle wie Cambridge Analytica. Vgl. a. das Kriterium des Bereithaltens für eine Einordnung als Diensteanbieter im TMG bei: *Lorenz*, VuR 2014, 83, 85 f.

[170] Zu denken ist hier insb. an Facebook und Twitter.

[171] Eventuell sogar als rechtliche Pflicht.

[172] Vgl. *Wagner*, ZD 2018, 307, 310.

[173] Vgl. *Hacker*, MMR 2018, 779, 781 f. zum Zu-Eigen-Machen im Rahmen der persönlichkeitsrechtlichen Störerhaftung. Vgl. *Wielsch*, RW 2019, 84, 100, 103, 105 zur Verantwortungssphäre von Intermediären.

[174] Vgl. *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users, 13.04.2021, Rn. 21.

[175] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 17.

[176] Dazu unten.

[177] Dazu: Kapitel 5 F. „Datenschutzrechtliche Beihilfe“.

[178] *Nebel*, RdV 2019, 9, 10; *Wagner*, ZD 2018, 307, 310. So müssten etwa im Falle der Löschung der Inhaltsdaten durch den Nutzer diese a. tatsächlich vom Anbieter gelöscht werden.

Verantwortlichen ebenso verwunderlich, wenn in diesem Szenario eine Entscheidung über die wesentlichen Elemente der Mittel vorausgesetzt würde und damit ein weisungsgebundener Auftragsverarbeiter vorliegen würde, ein nicht weisungsgebundener gemeinsam Verantwortlicher hingegen nicht. Denn ein weisungsgebundener Auftragsverarbeiter würde eindeutig für die Verarbeitung der Inhaltsdaten verantwortlich bleiben, wie sich aus ErwGr 18 S. 3 DSGVO ergibt. Erkennbar wird hier eines der schweren Defizite in der Verantwortlichkeitskonzeption des aktuellen Datenschutzrechts.[179]

Golland hingegen hält ein wechselseitiges Billigungsverhältnis der Zwecke für nicht ausreichend für eine gemeinsame Verantwortlichkeit und will in der Rechtssache Fashion ID[180] das zusätzliche Tatbestandselement des wirtschaftlichen Interesses bzw. „positiven wirtschaftlichen Wirkungszusammenhangs" als Einschränkung der gemeinsamen Verantwortlichkeit erkannt haben.[181] Somit nimmt er mangels wirtschaftlichen Interesses keine gemeinsame Verantwortlichkeit des Nutzers an, kommt aber letztlich zum selben Ergebnis wie bei Anwendung der Haushaltsausnahme. Als Voraussetzung für eine gemeinsame Verantwortlichkeit scheint dieser positive wirtschaftliche Wirkungszusammenhang allerdings ungeeignet und auch systematisch fehl am Platz. Die DSGVO trennt weder zwischen öffentlichen und nicht-öffentlichen Verantwortlichen noch zwischen kommerziellen und nicht-kommerziellen Akteuren. Ausnahmen werden positiv definiert und nicht anhand von Tatbestandselementen indirekt berücksichtigt.[182] So wäre ErwGr 18 S. 3 DSGVO im Rahmen dieses Verständnisses überflüssig. Notwendig erscheint der positive wirtschaftliche Wirkungszusammenhang als weitere Voraussetzung einer gemeinsamen Verantwortlichkeit nur dann, wenn man davon ausgeht, dass die Haushaltsausnahme durch die gemeinsame Verantwortlichkeit mit einem nicht privilegierten Akteur unanwendbar wird[183] oder aber erst gar nicht zur Anwendung kommt.

[179] Vgl. *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 16.
[180] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 80.
[181] *Golland*, ZD 2020, 397, 399.
[182] Vgl. *Brühann*, DuD[28] (2004), 201, 206.
[183] Möglicherweise wird dabei der Zweck der Glaubensgemeinschaft in EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 44 als überschreibend verstanden. Offensichtlich verfolgen die Mitglieder der Glaubensgemeinschaft aber denselben Zweck, der a. für sie isoliert keine Haushaltsausnahme bedeuten würde, vgl. die Erwägungen in *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, 6.

2. Praktikabilität einer gemeinsamen Verantwortlichkeit des Infrastrukturnutzers

Versteht man den Nutzer als gemeinsam Verantwortlichen für Verarbeitungsvorgänge in Bezug auf Inhalts- und Nutzungsdaten, stellt sich die Frage, inwiefern dieser überhaupt die Pflichten eines Verantwortlichen, insbesondere technischer Natur wie nach Art. 25 und 32 DSGVO, erfüllen könnte.[184] Um dieses Dilemma aufzulösen, bestünden drei Möglichkeiten. Zunächst könnte der Anbieter der Infrastruktur nachträglich Auftragsverarbeiter des Nutzers werden. Dies dürfte, wie bereits erwähnt, regelmäßig nicht praktikabel sein. Daneben könnte der Nutzer versuchen, auf eine Vereinbarung gem. Art. 26 Abs. 1 S. 2 DSGVO und allgemein auf die Erfüllung der datenschutzrechtlichen Pflichten seitens des Anbieters hinzuwirken.[185] Auch dies wirkt allerdings, allein im Hinblick auf die Verhandlungsposition eines durchschnittlichen Nutzers, utopisch. Zuletzt bestünde noch die Möglichkeit einer Privilegierung durch die Haushaltsausnahme. Damit würde die Anwendbarkeit der DSGVO für den Nutzer insgesamt entfallen. Unklar ist bislang aber, ob diese auch in Szenarien mit gemeinsam Verantwortlichen Anwendung findet. Ausgehend von der Feststellung des EuGH in dem Urteil zu der Rechtssache Wirtschaftsakademie, dass der bloße Umstand der Nutzung durch den Nutzer eines sozialen Netzwerks nicht zu seiner Verantwortlichkeit führen soll,[186] kann dies, wie dargestellt, nur sinnvoll über die Haushaltsausnahme erfolgen. Daneben scheint ErwGr 18 S. 3 DSGVO für die Anwendung der Haushaltsausnahme auch in den Fällen, in denen grundsätzlich eine gemeinsame Verantwortlichkeit vorliegen würde, zu sprechen. Denn der Verantwortliche oder Auftragsverarbeiter, der Instrumente für solche persönlichen oder familiären Tätigkeiten bereitstellt, soll ja weiterhin der DSGVO unterfallen. Abgesehen davon ist schließlich nicht erkennbar, warum der Kontext einer Verarbeitung nicht zwischen verschiedenen potenziell gemeinsam Verantwortlichen divergieren können sollte.[187]

Demnach bleibt die Haushaltsausnahme bei einer potenziellen gemeinsamen Verantwortlichkeit, bei der die Haushaltsausnahme nicht für alle gemeinsam Verantwortlichen anwendbar ist, anwendbar. Auch wenn unabhängig von der Haushaltsausnahme eine gemeinsame Verantwortlichkeit potenziell gegeben wäre, entfällt aufgrund der Haushaltsausnahme die Anwendbarkeit der DSGVO für den Nutzer insgesamt.

[184] *Wagner*, ZD 2018, 307, 310; zu den Pflichten a.: *Bock*, K&R 2019, 30, 31.
[185] *Wagner*, ZD 2018, 307, 310 f.
[186] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357, Rn. 35.
[187] So a.: *Wagner*, ZD 2018, 307, 311.

Ihn trifft also insbesondere keine Pflicht zum Abschluss der Vereinbarung und der Verteilung der Pflichten nach Art. 26 Abs. 1 S. 2 DSGVO.[188] Die Verantwortlichkeit fällt daher dem Anbieter insgesamt zu. Erachtet man hingegen die Haushaltsausnahme bei einer potenziellen gemeinsamen Verantwortlichkeit für nicht anwendbar, bestünde in Sachverhalten im digitalen Bereich sehr häufig eine gemeinsame Verantwortlichkeit von Nutzer und Anbieter.

3. Umfang der (gem-)einsamen Verantwortlichkeit

Geht man, entgegen der dargestellten Argumente, davon aus, dass eine gemeinsame Verantwortlichkeit von Nutzer und Anbieter für die Inhaltsdaten besteht, stellt sich in der Folge die Frage, auf welche Verarbeitungsvorgänge sich diese bezieht. Sinnvollerweise sind dies zumindest die Speicherung, Offenlegung (gegenüber Dritten) und Löschung der Daten. Insgesamt wären also alle Verarbeitungen der Inhaltsdaten erfasst, die sich auf der Infrastruktur des Anbieters abspielen und auf welche der Nutzer durch Interaktion mit der Infrastruktur Einfluss nehmen kann.[189]

4. Haushaltsausnahme und Auftragsverarbeiter

Liegt eine Weisungsgebundenheit des Anbieters vor, unterfällt der Nutzer aber der Haushaltsausnahme, stellt sich die Frage, ob noch eine Auftragsverarbeitung – mangels Verantwortlichkeit des Nutzers – vorliegt. Zu denken wäre hier etwa an Webmail-Dienste, Online-Nutzerkonten oder Cloud-Speicher, insbesondere wenn diese kostenpflichtig betrieben werden.[190] Der Unionsgesetzgeber hat sich mit dieser Frage, trotz Vorbringens der Art. 29-Datenschutzgruppe,[191] im Rahmen der DSGVO nicht auseinandergesetzt.

Denkbar ist zunächst, dass die Auftragsverarbeitung des Anbieters daran scheitert, dass kein Verantwortlicher als Auftraggeber vorhanden ist, der den Auftragsverarbeiter vertraglich binden würde und gegenüber dem er weisungsgebunden wäre. Folgt man diesem Ansatz, stellt sich die Folgefrage, ob der vermeintliche Auftragsverarbeiter, auch ohne einen Auftragsverarbeiterexzess gem. Art. 28 Abs. 10 DSGVO, zum Verantwort-

[188] Nicht nachvollziehbar ist daher die Ansicht von *Wagner*, ZD 2018, 307, 312, dass die Haushaltsausnahme zulasten der betroffenen Person geht.

[189] Also nicht anbieterseitige Analysen der Inhaltsdaten, etwa im Hinblick auf Content-Überprüfung, Werbungsanalysen oder Gruppen-/Kontaktvorschläge. Ein Überblick bei: *Golland*, ZD 2020, 397, 400 f.

[190] *Golland*, ZD 2020, 397, 400.

[191] *Artikel-29-Datenschutzgruppe*, Die Zukunft des Datenschutzes, 01.12.2009, 20 f.

lichen oder aber, ob er zum datenschutzrechtlichen Nullum wird. In der üblichen weiten Auslegung der Verantwortlichkeit scheint zumindest letzteres ausgeschlossen.[192] Aber auch die Verantwortlichkeit des Anbieters[193] scheint ein kaum gangbarer Weg, da dieser sich in Unkenntnis des Inhalts der personenbezogenen Daten kaum sinnvoll um eine Verarbeitungsrechtfertigung[194] sowie die potenzielle Geltendmachung von Betroffenenrechten kümmern könnte. Zudem wäre der Anbieter im Hinblick auf seine eigene Verarbeitungsrechtfertigung von der Anwendbarkeit der Haushaltsausnahme auf den Nutzer abhängig und müsste das Bestehen der Haushaltsausnahme konsequenterweise regelmäßig überprüfen.

Sinnvollerweise sollte hier eine Auftragsverarbeitung analog Art. 28 DSGVO angenommen werden,[195] auch in Ermangelung eines Verantwortlichen. Somit wäre der Auftragsverarbeiter gegenüber den Pflichten eines Verantwortlichen privilegiert und würde indirekt von der Haushaltsausnahme profitieren, was im Rahmen der Weisungsgebundenheit auch vertretbar erscheint. So wäre etwa keine eigene Verarbeitungsrechtfertigung des Auftragsverarbeiters erforderlich. Weitere Folge der analogen Anwendung wäre, dass ein Vertrag gem. Art. 28 Abs. 3 DSGVO zwischen dem durch die Haushaltsausnahme privilegierten Nutzer sowie dem Anbieter abzuschließen wäre.[196] Eine Schlechterstellung der betroffenen Person wäre bei der analogen Anwendung von Art. 28 DSGVO nicht ersichtlich. So spricht selbst ErwGr 18 S. 3 DSGVO davon, dass die DSGVO weiterhin für Auftragsverarbeiter gelten soll, auch wenn die Haushaltsausnahme für den Auftraggeber gilt. Die Verwendung des Begriffs des Auftragsverarbeiters wäre irreführend, wenn es sich faktisch um einen Verantwortlichen handeln würde.

VII. Fazit

Bei konsequenter Anwendung der Haushaltsausnahme lässt sich zumindest im Bereich der privaten Nutzung von fremder Infrastruktur durchaus eine Begrenzung der gemeinsamen Verantwortlichkeit erzielen. Problematisch erscheinen weniger die Konse-

[192] Vgl. *Monreal*, CR 2019, 797, Rn. 40; Simitis/Hornung/Spiecker/*Roßnagel*, Art. 2 DSGVO, Rn. 36.

[193] So noch in der 37. Edition: BeckOK DatenschutzR[37]/*Bäcker*, Art. 2 DSGVO, Rn. 23.

[194] *Golland*, ZD 2020, 397, 400 weist hier auf das besondere Problem von Art. 9 DSGVO hin.

[195] *Golland*, ZD 2020, 397, 400; Kühling/Buchner/*Kühling/Raab*, Art. 2 DS-GVO, Rn. 25; wohl a.: Simitis/Hornung/Spiecker/*Roßnagel*, Art. 2 DSGVO, Rn. 36.

[196] *Golland*, ZD 2020, 397, 400.

quenzen der Haushaltsausnahme für die Verantwortlichkeit als vielmehr die Voraussetzungen der Haushaltsausnahme selbst. Hier besteht für den EuGH in Ermangelung einer entsprechenden Reform der DSGVO noch einiges an Klärungsbedarf.

J. Störerhaftung und Zweckveranlasser

Im Vorfeld der Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit[197] war im deutschen Datenschutzrecht insbesondere strittig, ob eine zivilrechtliche Störerhaftung[198] oder eine öffentlich-rechtliche Inanspruchnahme als Zweckveranlasser möglich sei.[199] Dabei sollte die zivilrechtliche Störerhaftung bzw. die öffentlich-rechtliche Inanspruchnahme als Zweckveranlasser in Ermangelung einer originären Verantwortlichkeit des Akteurs greifen.[200] Folge dessen wäre dann aber keine Verpflichtung vergleichbar zum Verantwortlichen, sondern nur die Haftung auf Unterlassen[201] durch den Störer bzw. Zweckveranlasser. Aufgrund der Rechtsprechung des EuGH in der Rechtssache Fashion ID[202] ist hier von einem Ansatz de lege ferenda auszugehen, da entsprechende Normen gegebenenfalls erst noch verabschiedet werden müssten.

Bei der zivilrechtlichen Störerhaftung handelt es sich um eine spezielle Form der Haftung Dritter.[203] Rechtsfolge der zivilrechtlichen Störerhaftung ist (analog) § 1004 Abs. 1 BGB eine Beseitigung oder ein Unterlassen der Störung, also der Beeinträchtigung eines Rechtsguts, durch den Störer. Dabei basiert die Störerhaftung auf den Vorschriften zur Besitz- oder Eigentumsstörung. Störer ist – vereinfacht dargestellt –, wer ohne Täter oder Teilnehmer zu sein, in irgendeiner Weise willentlich und adäquat kausal zur Beeinträchtigung eines Rechtsguts beiträgt.[204] Aufgrund dieses weiten Anwendungsbereichs setzt die Haftung des Störers allerdings die Verletzung zumutbarer Verhaltenspflichten, insbesondere von Prüfpflichten, voraus.[205]

---

[197] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.
[198] Siehe etwa: *Spindler*, GRUR 2013, 996, 1003; *Golland*, K&R 2019, 533, 536 m.w.N.
[199] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1.
[200] So z.B.: *Alich/Nolte*, CR 2011, 741, 744 für die Haftung des Host-Providers.
[201] *Mantz*, ZD 2014, 62, 64 f.
[202] Dazu unten.
[203] Insgesamt kritisch zur Entwicklung der Rechtsprechung *Kremer*, https://www.cr-online.de/blog/2016/02/16/bgh-access-provider-sind-stoerende-nichtstoerer/ (abgerufen am 17.07.2024).
[204] BGH, Urteil vom 25.10.2011 – VI ZR 93/10 = GRUR 2012, 311, Rn. 21; *Wielsch*, RW 2019, 84, 99; *Hacker*, MMR 2018, 779, 780 f.
[205] BGH, Urteil vom 25.10.2011 – VI ZR 93/10 = GRUR 2012, 311, Rn. 22.

Der Zweckveranlasser im öffentlichen Recht[206] wiederum handelt zwar selbst rechtmäßig, da er mit seinem Verhalten nicht die Schwelle zur Eröffnung einer Gefahr überschreitet. Allerdings setzt der Zweckveranlasser durch sein Verhalten eine Kausalkette in Gang, an deren Ende eine andere Person die Gefahrenschwelle in ihr zurechenbarer Weise überschreitet. Das Verhalten des Zweckveranlasser ist dabei kausal im Sinne einer conditio-sine-qua-non-Kausalität für die entstandene Gefahr. Der Zweckveranlasser veranlasst objektiv also die Überschreitung der Gefahrenschwelle durch Dritte. Beispielhaft für den Zweckveranlasser steht die Nutzung einer anzüglichen Schaufensterreklame, die einen Massenauflauf vor dem Geschäft verursacht, der wiederum den Verkehr gefährdet. Aufgrund ihres weiten Anwendungsbereichs wird die Rechtsfigur des Zweckveranlassers allerdings durch ein objektives oder ein subjektives Zurechnungselement eingeschränkt. So muss entweder zwischen dem Verhalten des Zweckveranlassers und der Gefahr objektiv ein erkennbarer Wirkungs- und Verursachungszusammenhang bestehen oder der Zweckveranlasser muss diese Gefahr subjektiv wenigstens gebilligt haben.[207]

I. Raum für Störerhaftung und Zweckveranlasser?

Die Möglichkeit einer Störerhaftung wird vor allem in Verarbeitungsszenarien erwogen, in denen sich ein Akteur einer fremden Infrastruktur bedient, diese aber mangels Auftragsverarbeitung nicht hinreichend kontrollieren kann. Diese Problematik zeigt sich etwa in den Sachverhalten, die den Urteilen in den Rechtssachen Wirtschaftsakademie und Fashion ID zugrunde lagen.[208] Daher beziehen sich die Vorlagefragen des BVerwG[209] in der Rechtssache Wirtschaftsakademie auch auf eine „Auswahlverantwortlichkeit", die des OLG Düsseldorf[210] in der Rechtssache Fashion ID auf eine Störerhaftung. Damit sollen Verarbeitungsszenarien erfasst werden, in denen keine Verantwortlichkeit eines Akteurs bestehe, dieser Akteur aber in gewisser Weise mit der maßgeblichen Verarbeitung zusammenhänge.[211] Ob aber eine Verantwortlichkeit vor-

[206] Hierzu: *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 127 ff.

[207] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 10 m.w.N.

[208] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[209] BVerwG, Beschluss (Vorlage EuGH) vom 25.02.2016 – 1 C 28.14 = K&R 2016, 437, 438 Vorlagefrage 2.

[210] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 42 Vorlagefrage 3.

[211] *Piltz*, K&R 2014, 80, 82.

liegt, hängt wiederum davon ab, wie man die Voraussetzungen einer Verantwortlichkeit, insbesondere einer gemeinsamen Verantwortlichkeit, versteht.[212] Maßgebliche Fragen sind dabei, was einen Entscheidungsbeitrag darstellt und wozu dieser vorliegen muss. Unproblematisch dürfte für eine datenschutzrechtliche Störerhaftung hingegen regelmäßig als Voraussetzung der willentliche und adäquat kausale Beitrag eines vermeintlichen Störers sein.[213] Dieser wäre, sofern man eine gemeinsame Verantwortlichkeit ablehnt, in der Rechtssache Wirtschaftsakademie in der Eröffnung der Fanpage, in der Rechtssache Fashion ID in der Einbindung des Social Plugins zu sehen.

Die Möglichkeit der Störerhaftung eines Akteurs neben der Verantwortung eines Verantwortlichen wurde vor allem mit dem Argument zurückgewiesen, dass durch mitgliedstaatliche Sonderwege der Grundsatz der Vollharmonisierung der DSRL gem. ErwGr 8 gefährdet sei.[214] Zudem sei die Störerhaftung weder systematisch noch historisch zu begründen.[215] Im Rahmen von aufsichtsbehördlichen Maßnahmen käme eine zivilrechtliche Störerhaftung nicht in Frage, da sie systematisch dem Subordinationsverhältnis des vermeintlichen Störers gegenüber der Aufsichtsbehörde widerspreche.[216] Zudem würde die Annahme einer Störerhaftung bei aufsichtsbehördlichen Maßnahmen, mangels Verweises des Datenschutzrechts auf zivilrechtliche Haftungsnormen, dem Bestimmtheitsgebot widersprechen.[217]

Hinsichtlich des Zweckveranlassers wiederum soll aufgrund des Definitionselements der Entscheidung des Verantwortlichen gem. Art. 4 Nr. 7 DSGVO kein Raum hierfür mehr bestehen.[218] Teilweise wird der Zweckveranlasser auch als unzulässige Einschränkung des Zieles des freien Datenverkehrs aus Art. 1 Abs. 3 DSGVO zurückgewiesen.[219] Zudem könnten durch einen Rückgriff auf die ordnungsrechtlichen Störer die regulären Zuständigkeiten der Aufsichtsbehörden umgangen werden.[220] Nach deutschem Verständnis seien die Aufsichtsbehörden nämlich aufgrund ihrer völligen Unabhängigkeit keine regulären Wirtschaftsaufsichtsbehörden und könnten deshalb auch nicht auf die ordnungsrechtlichen Störer zurückgreifen.[221]

---

[212] Vgl. etwa *Piltz*, K&R 2014, 80, 83. Vgl. a. *Moos/Rothkegel*, MMR 2018, 596, 598 f.

[213] *Piltz*, K&R 2014, 80, 83 f.

[214] *Piltz*, K&R 2014, 80, 82.

[215] *Piltz*, K&R 2014, 80, 84 f.; vgl. a. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 317 ff.; Kritisch: *Mantz*, ZD 2014, 62, 64 f.

[216] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 10.

[217] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 10.

[218] *Fritzsche/Martini*, NVwZ-Extra[34] (2015), 1, 10 f. Kritisch a. insgesamt: *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 171 ff.

[219] *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, 2021, 90.

[220] *Lewinski/Herrmann*, ZD 2016, 467, 472.

[221] *Lewinski/Herrmann*, ZD 2016, 467, 472.

II. Rechtsprechung des EuGH

Die Ablehnung einer weiteren Art der Haftung neben der Verantwortlichkeit wurde in den Vorinstanzen zum Urteil des EuGH in der Rechtssache Wirtschaftsakademie deutlich. So verneinte das OVG Schleswig eine Übertragung der zivilrechtlichen Störerhaftung auf die Eingriffsverwaltung.[222] Ebenso verneinte es einen Rückgriff auf einen Störer nach den allgemeinen Regelungen des Gefahrenabwehrrechts, da im Rahmen der bestehenden Verantwortlichkeiten keine Schutzlücke bestünde.[223]

Der EuGH scheint im Hinblick auf die DSRL, und damit mutmaßlich auch für die DSGVO, eine andere Linie zu verfolgen. Zwar lässt er die Vorlagefrage bezüglich der Möglichkeit einer Störerhaftung,[224] sofern keine Verantwortlichkeit gegeben sei, mit Verweis auf die Beantwortung der Vorlagefrage bezüglich der Verantwortlichkeit selbst, offen.[225] Schließlich liege ja bereits eine gemeinsame Verantwortlichkeit vor. Allerdings stellt er in der Beantwortung der Vorlagefrage zur Verantwortlichkeit, auf die er bezüglich der Vorlagefrage zur Störerhaftung ja verweist,[226] fest, dass eine zivilrechtliche Haftung auf Basis nationalen Rechts bei fehlender Verantwortlichkeit, etwa hinsichtlich vor- oder nachgelagerter Verarbeitungsvorgänge, durchaus möglich sei.[227] Kurzum: eine Haftung für Verarbeitungsvorgänge, für die keine Verantwortlichkeit besteht, ist nach nationalem Recht möglich und nicht etwa durch eine vermeintlich abschließende Regelung des allgemeinen Adressaten der DSRL, also des Verantwortlichen, ausgeschlossen.[228] *Golland* hat trotz dieser Ausführungen des EuGH Bedenken hinsichtlich einer Anwendung der zivilrechtlichen Störerhaftung im Datenschutzrecht. Denn Art. 82 DSGVO sei hinsichtlich der Haftung abschließend und die An-

[222] OVG Schleswig, Urteil vom 04.09.2014 – 4 LB 20/13 = ZD 2014, 643, 644.

[223] OVG Schleswig, Urteil vom 04.09.2014 – 4 LB 20/13 = ZD 2014, 643, 645.

[224] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 42 Vorlagefrage 3.

[225] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 84 ff.

[226] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 86: „In Anbetracht der Antwort auf die zweite Frage braucht die dritte Frage nicht beantwortet zu werden."

[227] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74: „Dagegen kann, unbeschadet einer etwaigen insoweit im nationalen Recht vorgesehenen zivilrechtlichen Haftung, diese natürliche oder juristische Person für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder die Zwecke noch die Mittel festlegt, nicht als im Sinne dieser Vorschrift verantwortlich angesehen werden."

[228] *Kremer*, CR 2019, 676, Rn. 14; S/J/T/K/*Kremer*, Art. 26 DSGVO, Rn. 51; *Monreal*, CR 2019, 797, Rn. 47.

wendung der Störerhaftung bei einem Sonderordnungsrecht wie dem Datenschutzrecht stoße auf rechtsstaatliche Bedenken.[229] Insofern sieht er die Frage, ob die Anwendung der Störerhaftung im Datenschutzrecht möglich sei, als weiterhin offen an.[230] So unbefriedigend kurz die Ausführungen des EuGH sein mögen, lassen sie aber trotzdem eindeutig erkennen, dass die DSRL keine abschließende Regelung für eine Haftung trifft. Ebenso hatte die Art. 29-Datenschutzgruppe bereits 2010 festgehalten, dass es möglich sei „[...] dass nationale Rechtsvorschriften eine strafrechtliche oder verwaltungsrechtliche Haftung nicht nur für den für die Verarbeitung Verantwortlichen vorsehen, sondern auch für jede andere Person, die gegen das Datenschutzrecht verstößt."[231]

1. Folgefragen

Da der EuGH die Vorlagefrage zur Störerhaftung effektiv in einem Nebensatz abhandelt, stellt sich eine Fülle an Folgefragen.[232] Am vordringlichsten scheint dabei die Frage nach der potenziellen Reichweite einer solchen zivilrechtlichen Haftung, also ob die vom EuGH explizit angesprochene zivilrechtliche Haftung nur einen Schadensersatz, ein Unterlassen oder weitere Pflichten umfasst. Neben dem Schadensersatz sollte dabei sinnvollerweise auch ein Unterlassen erfasst sein. Eine weitergehende Haftung hingegen erscheint zu unbestimmt.[233]

Zudem stellt sich die Frage, ob Grundlage für die Haftung dann immer noch ein datenschutzrechtliches Fehlverhalten oder etwas anderes, etwa eine Verletzung des Persönlichkeitsrechts,[234] ist. Es stellt sich also genau genommen die Frage, ob die vom EuGH erwähnte zivilrechtliche Haftung Bezug nimmt auf eine anderweitige Rechtsgutverletzung, also nicht des Datenschutzrechts,[235] oder aber eben nur die Konstruktion des Anspruchgegners, also des Störers, betrifft. Da der EuGH hinsichtlich der zivilrechtlichen Haftung auf der Verarbeitungskette vor- oder nachgelagerte Vorgänge Bezug nimmt, also auf datenschutzrechtliche Terminologie, erscheint es denkbar, dass dies nur die Konstruktion des Anspruchsgegners betrifft. Dies liegt auch deswegen

---

[229] *Golland*, K&R 2019, 533, 536.

[230] Kritisch zur fehlenden, eindeutigen Beantwortung bereits in der Rechtssache Wirtschaftsakademie: *Moos/Rothkegel*, MMR 2018, 596, 598 f.

[231] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 20 Fn. 15.

[232] Vgl. a. *Moos/Rothkegel*, MMR 2019, 584, 586.

[233] A. *Monreal*, CR 2019, 797, Rn. 47 sieht nur einen eingeschränkten Anwendungsbereich für die Störerhaftung.

[234] Bspw. § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG.

[235] Vgl. *Lewinski/Herrmann*, ZD 2016, 467, 472.

nahe, da die vom OLG Düsseldorf vorlegte Frage das deutsche Konzept der Störerhaftung betraf. Sofern der EuGH anderweitige Anspruchsgrundlagen im Blick hatte, die nicht nur die Konstruktion des Anspruchgegners, sondern auch das geschützte Rechtsgut bzw. das vorgeworfene Fehlverhalten betreffen, wäre dieser Nebensatz irreführend. Andererseits hält ErwGr 146 S. 4 DSGVO fest, dass die Schadensersatzregelungen der DSGVO einen Schadensersatz aufgrund Verstoßes gegen sonstiges Unions- und mitgliedstaatliches Recht unberührt lassen. Dies würde dann voraussetzen, dass es sich bei der zivilrechtlichen Haftung nach mitgliedstaatlichem Recht nicht um einen Verstoß gegen materielles Datenschutzrecht handelt. Inwiefern der diesem ErwGr zugrunde liegende Gedanke hier maßgeblich sein kann, bleibt vorerst allerdings unklar, da der EuGH nur zur Rechtslage nach DSRL entschieden hat.[236] Insgesamt stellt sich also die Frage, ob entsprechende mitgliedstaatliche Regelungen ein aliud zum Datenschutzrecht darstellen oder subsidiär wirken müssen.[237]

Eine weitere Frage stellt sich im Hinblick darauf, ob neben einer weitergehenden zivilrechtlichen Haftung auch Raum für eine öffentliche-rechtliche Haftung, etwa des Zweckveranlassers (als quasi-Äquivalent des zivilrechtlichen Störers) ist.[238] Geht man von einer weitgehenden Parallelität der Durchsetzung der DSGVO durch betroffene Personen und Aufsichtsbehörden hinsichtlich der materiellen Verpflichtung der Adressaten, also insbesondere des Verantwortlichen, aus, ist kaum nachvollziehbar, warum eine betroffene Person gegen einen Störer vorgehen könnte, einer Aufsichtsbehörde hingegen keine Maßnahmen gegen einen Zweckveranlasser möglich wären. Daher müsste eine Inanspruchnahme des öffentlich-rechtlichen Zweckveranlassers analog zur zivilrechtlichen Haftung eines Störers ebenso möglich sein. Denkbar wäre allerdings auch, dass der EuGH von vornherein keine Gleichwertigkeit der Durchsetzungsmöglichkeiten der betroffenen Person und der Aufsichtsbehörden voraussetzt. Insofern wäre die Möglichkeit einer Inanspruchnahme des Zweckveranlassers dann nicht systematisch notwendig.

2. Schlussanträge des Generalanwalts

Die Schlussanträge des Generalanwalts in der Rechtssache Fashion ID verhelfen diesen Fragen zu keiner weiteren Klärung. Denn der Generalanwalt hatte eine unionsweite

[236] Zustimmend zur Möglichkeit einer weitergehenden zivilrechtlichen Haftung m.w.N.: *Specht-Riemenschneider/Schneider*, GRUR Int 2020, 159, 161.

[237] Vgl. *Lauber-Rönsberg*, AfP 2019, 373, Rn. 45 f.

[238] Zum Rückgriff auf die Adressaten des allgemeinen Polizei- und Ordnungsrechts: Kapitel 5 K. Rückgriff auf Adressaten des allgemeinen Polizei- und Ordnungsrecht.

Harmonisierung der Haftung durch eine abschließende Regelung im Rahmen des Verantwortlichkeitsbegriffs vor Augen und schloss somit eine Störerhaftung aus.[239] Dabei scheint der Generalanwalt allerdings übersehen zu haben, dass durch die Störerhaftung (nach deutscher Konzeption) keineswegs der Störer selbst Verpflichteter der durch die DSRL vorgegebenen Pflichten würde, sondern er vielmehr nur ein Verhalten, das zu einem Datenschutzverstoß seitens eines Verantwortlichen führen würde, zu unterlassen hätte. Somit wäre also nur das die rechtswidrige Verarbeitung ermöglichende Verhalten seitens des Störers einzustellen. Eine Störerhaftung im Datenschutzrecht wäre also immer akzessorisch zu einer bestehenden Verantwortlichkeit. Kritikwürdig an einer Störerhaftung nach mitgliedstaatlichem Recht scheint allerdings durchaus die Gefahr der Rechtszersplitterung.[240] Wenn an einem so essenziellen Grundsatz des Datenschutzrechts wie der Frage des Adressaten je nach Mitgliedstaat unterschiedliche Regimes vorliegen, wird damit der Vollharmonisierungsansatz der DSGVO konterkariert. Wünschenswert, wenn auch unwahrscheinlich, wäre daher die Lösung einer solchen Haftung Dritter auf unionsrechtlicher Ebene.[241]

III. Fazit

Eine Störerhaftung oder eine Haftung als Zweckveranlasser auf der Basis mitgliedstaatlichen Rechts dürfte, sofern sich die angedeutete Rechtsprechung des EuGH bestätigen sollte, eine der wenigen kurzfristigen Möglichkeiten sein, einem zu weiten Verständnis der gemeinsamen Verantwortlichkeit entgegenzuwirken. Insofern besteht für potenziell „Verantwortliche" rechtspolitisch ein Dilemma. Wehren sie sich nicht gegen eine bestimmte Art der Inanspruchnahme durch betroffene Personen oder Aufsichtsbehörden, riskieren sie möglicherweise eine unberechtigte Inanspruchnahme. Wehren sie sich hingegen gegen diese Inanspruchnahme, stellt möglicherweise spätestens der EuGH eine reguläre Verantwortlichkeit fest. Langfristig bieten die Anwendung der Störerhaftung oder des Zweckveranlassers nach mitgliedstaatlichem Recht aber auch keine Lösung für die Defizite des Konzeptes der Verantwortlichkeit in der DSGVO, gerade auch im Hinblick auf den Verordnungscharakter der DSGVO. Sie können insoweit nur eine Zwischenlösung darstellen. Denkbar erscheint aber eine unionsrechtliche Fixierung des Konzeptes der Störerhaftung bzw. des Zweckveranlassers auch um

[239] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 110.
[240] *Moos/Rothkegel*, MMR 2019, 584, 586.
[241] Vgl. zur Einzelfallrechtsprechung bei der Störerhaftung *Kremer*, https://www.cr-online.de/blog/2016/02/16/bgh-access-provider-sind-stoerende-nichtstoerer/ (abgerufen am 17.07.2024).

technischen Entwicklungen kurzfristig begegnen zu können. Dies müsste dann aber in der DSGVO oder im sonstigen sekundären Unionsrecht normiert werden.

K. Rückgriff auf Adressaten des allgemeinen Polizei- und Ordnungsrecht

Da die bisherige Rechtsprechung des EuGH die Voraussetzung einer der Verarbeitung vor- oder nachgelagerten Haftung bislang nur angedeutet hat, sollte auch erwogen werden, ob Maßnahmen der Aufsichtsbehörden nur gegenüber dem Verantwortlichen oder Auftragsverarbeiter ergehen können. So lässt gerade die Beschränkung bzw. das Verbot einer Verarbeitung in Art. 58 Abs. 2 lit. f DSGVO keinen Adressaten erkennen. Dies steht im Gegensatz zu den übrigen Abhilfebefugnissen der Aufsichtsbehörden, die direkt oder indirekt einen Adressaten erwähnen. Mangels eines erkennbaren Adressaten wäre es daher denkbar, über den Verweis auf das mitgliedstaatliche Verfahrensrecht gem. Art. 58 Abs. 4 DSGVO auf die Adressaten des allgemeinen Polizei- und Ordnungsrechts zurückzugreifen. Da man den Verantwortlichen bereits als Verhaltensstörer im Hinblick auf eine rechtswidrige Verarbeitung verstehen kann, wäre vor allem an den oben erwähnten Zweckveranlasser als Sonderform des Verhaltensstörers sowie eine Inanspruchnahme nicht verantwortlicher Personen zu denken. Die Inanspruchnahme nicht verantwortlicher Personen wäre allerdings, wie etwa in § 7 POG RLP, stark eingeschränkt. Sofern die Anwendung der Adressaten des allgemeinen Polizei- und Ordnungsrechts möglich ist, wäre dann aber eine gemeinsame Verantwortlichkeit in diesen Fällen abzulehnen. Durch einen solchen Rückgriff auf die Adressaten des allgemeinen Polizei- und Ordnungsrecht könnte die gemeinsame Verantwortlichkeit in Fällen, in denen ein Akteur klar überwiegend verantwortlich ist, überflüssig werden. Hinsichtlich der erfassten Akteure wäre an dieselben Verarbeitungsszenarien wie bei der Auswahlverantwortlichkeit oder in den Urteilen[242] in den Rechtssachen Wirtschaftsakademie und Fashion ID zu denken. Dieser Ansatz ist bereits nach geltendem Recht denkbar.

[242] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

I. Aufsichtsbehördliche Maßnahmen als Gefahrenabwehrrecht

Voraussetzung für einen Rückgriff auf die Adressaten des allgemeinen Polizei- und Ordnungsrechts wäre zunächst, dass es sich beim Datenschutzrecht, jedenfalls hinsichtlich der aufsichtsrechtlichen Maßnahmen, um Gefahrenabwehrrecht im Sinne der deutschen Systematik handelt. Teilweise werden die Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich als Wirtschaftsaufsichtsbehörden[243] bezeichnet, teilweise auch als „Ordnungsbehörde plus"[244]. Sofern diese Bezeichnung trägt, handelt es sich bei der Tätigkeit der Aufsichtsbehörden um besonderes Ordnungs- bzw. Gefahrenabwehrrecht.

1. Entgegenstehende unionsrechtliche Systematik?

Eine Einordnung des Datenschutzrechts als besonderes Gefahrenabwehrrecht im Rahmen der deutschen Systematik wäre allerdings dann nicht möglich, wenn bereits eine eigene unionsrechtliche Systematik bestehen würde. Während eine Einordnung nach mitgliedstaatlicher Systematik im Rahmen der Richtliniennatur der DSRL noch unproblematisch war,[245] ist dies aufgrund der Verordnungsnatur der DSGVO nicht ohne weiteres möglich. Denn im Gegensatz zur DSRL gilt die DSGVO als Verordnung unmittelbar. Daher muss für eine Anwendung der mitgliedstaatlichen Systematik ein Bezug der aufsichtsbehördlichen Tätigkeit zum mitgliedstaatlichen Recht bestehen.

Gem. Art. 51 Abs. 1 DSGVO sieht jeder Mitgliedstaat vor, dass eine oder mehrere Behörden für die Überwachung der Anwendung der DSGVO zuständig sind. Diese Festlegung der zuständigen Behörde geschieht gem. Art. 54 Abs. 1 DSGVO durch Rechtsvorschriften des Mitgliedstaates, also nicht, abseits der Vorgaben in Kapitel VI[246]

---

[243] So etwa: Auernhammer/*Lewinski*, § 38 BDSG a.F., Rn. 1 m.w.N. Verwunderlich ist dort, dass in Rn. 2 die Datenschutzaufsicht als Sonderordnungsbehörde bezeichnet wird; uneingeschränkt noch: *Lewinski*, RdV 2001, 275, 279 f.; inwiefern § 38 Abs. 1 S. 6 a.E. BDSG a.F. einen Anhaltspunkt für eine Einordnung als Gewerbeaufsicht bot, mag dahingestellt sein, eine Überschneidung von Aufsichtsbereichen der Datenschutz- und Gewerbeaufsicht ist jedenfalls nicht auszuschließen, wie auch § 38 Abs. 7 BDSG a.F. andeutete. *Masing* etwa vergleicht die datenschutzrechtliche Aufsicht mit der Gewerbeaufsicht, allerdings auch der Aufsicht im Umweltrecht: *Masing*, NJW 2012, 2305, 2311; *Reimer*, DÖV 2018, 881, 881 schließlich bezeichnet das Datenschutzrecht im nicht-öffentlichen Bereich als im Wesentlichen als Teil des öffentlichen Wirtschaftsrechts.

[244] *Brink* sieht Aufgaben über eine klassische Polizeiverwaltungsbehörde hinaus: BeckOK DatenschutzR[28]/*Brink*, § 38 BDSG a.F., Rn. 5; *Lepper/Wilde*, CR 1997, 703, 705 hingegen sieht keine qualitativen Unterschiede zur Bauaufsicht.

[245] *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 203 f. problematisiert dies im Kontext der Aufsichtsbehörde überhaupt nicht, auch wenn unionsrechtliche Bedenken generell durchaus vorhanden sind: ebd., 199 ff.

[246] „Unabhängige Aufsichtsbehörden".

der DSGVO, durch eine unionsrechtliche Anordnung. Daneben erfolgt nach Art. 58 Abs. 4 DSGVO die Ausübung der der Aufsichtsbehörde im Rahmen von Art. 58 DSGVO übertragenen Befugnisse nach dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta. Dieser Verweis ist auch dadurch bedingt, dass es trotz gewisser unionsrechtlicher Maßgaben kein einheitliches europäisches Verwaltungsverfahrensrecht gibt.[247] Schließlich kann ein Mitgliedstaat gem. Art. 58 Abs. 6 DSGVO der Aufsichtsbehörde auch weitere Befugnisse zuweisen. Diese Verweise auf das mitgliedstaatliche Recht verdeutlichen, dass es sich bei der Aufsichtsbehörde nicht um ein unionsrechtliches Spezifikum handelt, sondern eine Behörde, die sich unter den Vorgaben der DSGVO in das mitgliedstaatliche Recht einfügt.[248] Dabei wird die Kohärenz der mitgliedstaatlichen Umsetzung mit der DSGVO und sonstigem Unionsrecht durch die Notifizierungspflicht in Art. 51 Abs. 4 DSGVO sichergestellt. Insgesamt ist die Grundkonzeption der Aufsichtsbehörde nach Art. 52 und 55 Abs. 1 DSGVO also die einer unabhängigen und territorial begrenzten Behörde. Die mitgliedstaatliche Normierung der Datenschutzaufsicht wird zwar insgesamt durch die Vorgaben der Art. 51 ff. DSGVO eingeschränkt.[249] Dies kommt allerdings nicht einer eigenen unionsrechtlichen Systematik gleich.[250] Daher steht das Unionsrecht einer Einordnung des Datenschutzrechts in seiner aufsichtsbehördlichen Dimension nach deutscher Systematik nicht entgegen.[251]

[247] Ehmann/Selmayr/*Selmayr*, Art. 58 DS-GVO, Rn. 5, 33; ebenso der EuGH zur DSRL: EuGH, Urteil vom 01.10.2015 – C-230/14 (Weltimmo) = ZD 2015, 580, Rn. 50.

[248] So a.: Ehmann/Selmayr/*Selmayr*, Art. 54 DS-GVO, Rn. 4. Es handelt sich formal um nationale Behörden, die aber funktional zu einer dezentralen Unionsbehörde werden. Ebenso Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 5: Art. 58 DSGVO kann nicht autark, also ohne Bezug zur mitgliedstaatlichen Rechtsordnung, angewandt werden.

[249] Die DSGVO greife dabei tief in Fragen der nationalen Verwaltungsorganisation ein: Ehmann/Selmayr/*Selmayr*, Art. 51 DS-GVO, Rn. 1. Ebenso sei Bezugspunkt der nationalen Aufsichtsbehörden primär das Unionsrecht: Ehmann/Selmayr/*Selmayr*, Art. 58 DS-GVO, Rn. 1.

[250] Vgl. Taeger/Gabel/*Grittmann*, Art. 51 DSGVO, Rn. 2, 6.

[251] Vgl. zum mitgliedstaatlichen Spielraum Gola/Heckmann/*Nguyen/Stroh*, Art. 54 DSGVO, Rn. 1 m.w.N. mit Verweis auf Art. 4 Abs. 2 S. 1 AEUV. Ebenso Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 7, 101, der bereits eine Einordnung als besondere Ordnungsbehörde vornimmt.

2. Einordnung nach deutscher Systematik

a) Ordnungsbehörde und Ordnungsrecht

Der Begriff der allgemeinen Ordnungsbehörde[252] bezeichnet Organe bzw. Behörden, die Aufgaben der Gefahrenabwehr im weiteren Sinne[253] wahrnehmen.[254] Bei der Datenschutzaufsicht handelt es sich jedoch um eine Behörde mit sehr spezifischen Aufgaben. Gem. Art. 51 Abs. 1 DSGVO sind die Datenschutzaufsichtsbehörden für die Überwachung der DSGVO und damit den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie die Erleichterung des freien Verkehrs personenbezogener Daten in der EU zuständig. Aufgrund dieser spezifischen Aufgaben kann man die Datenschutzaufsicht als Sonderordnungsbehörde einordnen.[255] Die Einordnung einer Behörde als Sonderordnungsbehörde folgt in der Praxis allerdings keiner erkennbaren Systematik.[256] Üblicherweise wird der Begriff der Sonderordnungsbehörde dahingehend verstanden, dass es sich um eine Behörde handelt, die sich außerhalb der allgemeinen polizei- und ordnungsbehördlichen Verwaltung befindet und der durch besondere Rechtsvorschriften Aufgaben der Gefahrenabwehr zugewiesen werden.[257] Dies ergibt sich etwa aus § 103 Abs. 2 POG RLP oder § 90 S. 1 HSOG. Ebenso wie die allgemeinen Ordnungsbehörden können Sonderordnungsbehörden potenziell auf die Befugnisse der allgemeinen Ordnungsbehörden zurückgreifen.[258] Dies gilt allerdings dann nicht, wenn gegenüber diesen Befugnissen lex specialis-Regelungen für die Sonderordnungsbehörden bestehen.[259] Dabei stellt sich dann aber wiederum die Frage, ob diese lex specialis-Regelungen abschließend sind.

---

[252] Teilweise a. als allgemeine Polizeibehörde bezeichnet (etwa § 1 Abs. 1 SächsPBG).

[253] In Abgrenzung zur Vollzugspolizei (etwa §§ 1, 2 SächsPVDG).

[254] Vgl. etwa § 1 Abs. 1 S. 1 POG RLP.

[255] So a.: *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 205; *Schmeling*, DuD 2002, 351, 352 f., 355; deutlich: *Stentzel*, PinG 2016, 45, 46.

[256] *Rachor/Roggan*, C. Organisation der Sicherheitsbehörden und Geheimdienste in Deutschland, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 25 mit Beispielen für Sonderordnungsbehörden.

[257] So: *Rachor/Roggan*, C. Organisation der Sicherheitsbehörden und Geheimdienste in Deutschland, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 25.

[258] *Rachor/Roggan*, C. Organisation der Sicherheitsbehörden und Geheimdienste in Deutschland, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 26; spezifisch zum Datenschutz: *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 202 f.

[259] *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 203; *Erbguth/Mann/Schubert*, Besonderes Verwaltungsrecht, [13]2019, Rn. 678.

Die Gefahrenabwehr,[260] die von Ordnungsbehörden wahrgenommen wird, orientiert sich an der Abwehr von Gefahren,[261] also dem Verhindern von Schäden an Rechtsgütern.[262] Die DSGVO dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie dem freien Verkehr solcher Daten.[263] Dieser Schutz von Personen und der sie betreffenden personenbezogenen Daten findet sich als Grundrecht in Art. 8 Abs. 1 GRCh wieder. Liegt ein Verstoß gegen die DSGVO vor, ist damit zumindest das Schutzgut der öffentlichen Sicherheit verletzt. Zudem kann potenziell auch ein Schaden an Rechtsgütern der betroffenen Personen vorliegen. Die Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen hat gem. Art. 57 Abs. 1 lit. a DSGVO die (Datenschutz-)Aufsichtsbehörde.[264] Deren Eingriffsbefugnisse, etwa in Art. 58 Abs. 2 lit. b DSGVO, verwenden zwar nicht explizit den Begriff Gefahr oder Verstoß. Dadurch, dass ein Verarbeitungsvorgang mit der Verordnung in Einklang zu bringen ist, setzen die Eingriffsbefugnisse aber voraus, dass solche Verstöße bestehen.[265] Bei den durch die Aufsichtsbehörde festgestellten Verstößen handelt es sich also um bestehende oder unmittelbar bevorstehende Gefahren.[266]

Kennzeichnend für eine Ordnungsbehörde ist traditionell eine allgemeine Eingriffsermächtigung oder Generalklausel,[267] beispielsweise § 9 POG RLP oder § 59 Abs. 1 S. 1 LBauO RLP. Eine solche bestand für die Datenschutzaufsicht nach altem Recht[268]

[260] Vgl. insgesamt *Wißmann*, § 14 Grundmodi der Aufgabenwahrnehmung, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, [3]2022, Rn. 86 ff.

[261] *Graulich*, E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 121 ff.

[262] *Wißmann*, § 14 Grundmodi der Aufgabenwahrnehmung, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, [3]2022, Rn. 90.

[263] Letzteres wird vor allem durch die einheitlichen Vorgaben der DSGVO gewährleistet. Vgl. etwa VG Mainz, Urteil vom 20.02.2020 – 1 K 467/19.MZ, Rn. 28 zu den Verarbeitungsrechtfertigungen.

[264] Zu diesen Aspekten Dürig/Herzog/Scholz[103.]/*Möstl*, Art. 87e GG, Rn. 149 als traditionelle präventive und repressive ordnungsbehördliche Maßnahmen.

[265] Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 34.

[266] *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 204 zum BDSG a.F.; unklarer: *Stentzel*, PinG 2016, 45, 46.

[267] Näher hierzu: *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 19, 23, 25, 84, 183; *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 177; *Graulich*, E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 87.

[268] Eingriffsermächtigungen der Aufsichtsbehörden bestehen allerdings erst seit dem BDSG 1990, vgl. Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 62 ff. Ursprünglich galt dies a. nur im Hinblick auf technische oder organisatorische Mängel.

gem. § 38 Abs. 5 S. 1 BDSG a.F.[269] Die in Art. 58 Abs. 2 DSGVO geregelten Abhilfebefugnisse enthalten keine vergleichbare allgemeine Eingriffsermächtigung. Allerdings kann man auch die Gesamtheit der Abhilfebefugnisse als eine solche Eingriffsermächtigung verstehen.[270] Aufgrund der Weite und des Detailgrades der aufsichtsbehördlichen Befugnisse in der DSGVO nimmt etwa *Ziebarth* insgesamt eine besondere Ordnungsbehörde[271] an.[272] Der Unionsgesetzgeber selbst will, wie sich aus ErwGr 150 S. 1 DSGVO ergibt, die Abhilfebefugnisse der Aufsichtsbehörden aus Art. 58 Abs. 2 DSGVO als verwaltungsrechtliche Sanktion verstanden wissen. Zudem weisen Verwaltungsakte der Datenschutzaufsichtsbehörden eine ordnungsrechtliche Qualität auf.[273]

Ein weiteres Indiz für die Einordnung der DSGVO als Ordnungsrecht findet sich in Art. 5 Abs. 1 lit. a DSGVO i.V.m. Art. 6 Abs. 1 DSGVO. Das dort normierte Erfordernis der Rechtmäßigkeit der Verarbeitung im Rahmen der Verarbeitungsrechtfertigungen von Art. 6 Abs. 1 DSGVO wird häufig als „Verbot mit Erlaubnisvorbehalt" bezeichnet.[274] Es findet sich auch in Art. 8 Abs. 2 GRCh wieder. Dieser Begriff ist allerdings irreführend.[275] Während beim Verbot mit Erlaubnisvorbehalt eine ex-ante-Prüfung der begehrten Handlung stattfindet, findet im Datenschutzrecht nur gegebenenfalls eine ex-post-Prüfung statt.[276] Die Verarbeitung personenbezogener Daten setzt, mit Ausnahme von Art. 36 Abs. 5 DSGVO, keine Genehmigung oder Erlaubnis einer

[269] *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 191 ff.; *Schmeling*, DuD 2002, 351, 352; *Stentzel*, PinG 2016, 45, 48; a.A. Auernhammer/*Lewinski*, § 38 BDSG a.F., Rn. 72 und *Lewinski*, RdV 2001, 275, 275 sowohl vor als a. nach dem BDSG 2001. Nicht nachvollziehbar ist v.a. die (scheinbare) Ansicht von Lewinskis, das Fehlen von bestimmten Befugnissen (etwa der Schließung von Betrieben) disqualifiziere die Klausel als aufsichtsrechtliche Generalklausel. Begründet schien diese Reduktion vielmehr im Schutzzweck des Gesetzes, der sich aus § 1 Abs. 1 BDSG a.F. ergab und vor dem Umgang mit Daten, nicht der Tätigkeit eines Gewerbes schützte.

[270] Vgl. die Parallelargumentation zu § 38 BDSG a.F. bei *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 204 f. Zu den Strukturelementen einer Ordnungsnorm: *Schmidt-Preuß*, Kollidierende Privatinteressen im Verwaltungsrecht, 1992, 216 ff.

[271] Bzw. Sonderpolizeibehörde.

[272] Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 7, 98. Die aufsichtsbehördlichen Befugnisse der DSGVO sollen dabei allerdings kraft Spezialität die Möglichkeit der allgemeinen Polizei- und Ordnungsbehörden einzuschreiten verdrängen.

[273] Vgl. Simitis/Hornung/Spiecker/*Polenz*, Art. 58 DSGVO, Rn. 7. VG Oldenburg, Urteil vom 12.03.2013 – 1 A 3850/12 = ZD 2013, 296, 297 jedenfalls für das BDSG a.F. Vgl. zur Ermächtigungsgrundlage in § 38 Abs. 5 BDSG a.F. auch BT-Drs. 16/12011, S. 44. Zur Notwendigkeit: *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 459.

[274] Simitis/Hornung/Spiecker/*Roßnagel*, Art. 5 DSGVO, Rn. 36 m.w.N.

[275] Ausführlich: Simitis/Hornung/Spiecker/*Roßnagel*, Art. 5 DSGVO, Rn. 36.

[276] Simitis/Hornung/Spiecker/*Roßnagel*, Art. 5 DSGVO, Rn. 36.

Aufsichtsbehörde voraus.[277] Der Verantwortliche ist im Rahmen seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO vielmehr gehalten die Rechtmäßigkeit i.S.v. Art. 6 Abs. 1 DSGVO selbst nachzuweisen.[278] Daher wird diese Regelungsmethode unter anderem auch als Verbotsgrundsatz bezeichnet.[279] Dieser Verbotsgrundsatz, also der Zwang zu einer Verarbeitungsrechtfertigung, weist nichtsdestotrotz eine gewisse Nähe zum Ordnungsrecht auf.[280]

b) Aufsicht sui generis?

Vereinzelt wird die Datenschutzaufsicht in der Literatur als Aufsicht sui generis verstanden.[281] Dies wird unter anderem damit begründet, dass es sich beim Beschwerdeverfahren gegenüber den Aufsichtsbehörden um eine Art Petitionsrecht handeln soll.[282] Diese Analogie zur Petition bezieht sich maßgeblich auf einen Beschluss des VGH München, in dem dieser entschieden hatte, dass eine Eingabe an den Landesbeauftragten für Datenschutz kein Verfahren i.S.v. Art. 29 Abs. 1 BayVwVfG in Gang setze. Der VGH begründete dies damit, dass der Landesbeauftragte gegenüber einer Behörde (nach damaligem Recht)[283] weder eine Weisung noch einen Verwaltungsakt erlassen könne. Zudem gäbe es keinen Anspruch seitens der betroffenen Person gegenüber dem Landesbeauftragten auf die Beanstandung einer Behörde.[284]

Mit der DSGVO lässt sich dieses Verständnis nicht weiter aufrechterhalten.[285] So haben betroffene Personen gem. Art. 77 Abs. 1 DSGVO unbeschadet eines anderweitigen verwaltungsrechtlichen Rechtsbehelfs ein Recht auf eine Beschwerde bei einer

---

[277] Vgl. *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 155 ff. zur Verantwortlichkeitszuschreibung als Form von Risikomanagement.

[278] Eingehend: *Simitis*, CR 1987, 602, 611; *Walz*, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, 2000, 455. *Burkert*, 2.3 Internationale Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, Rn. 17 bezeichnet dies als „Selbsteinschätzungsmodell".

[279] BeckOK DatenschutzR[28]/*Bäcker*, § 4 BDSG a.F., Rn. 3 ff.

[280] Es bieten sich Vergleiche zu genehmigungsfreien Bauvorhaben wie etwa in § 62 LBauO RLP an.

[281] So: *Tinnefeld/Petri*, MMR 2010, 157, 157; Kühling/Buchner/*Boehm*, Art. 51 DS-GVO, Rn. 10 f.

[282] VGH München, Beschluss vom 10.03.1988 – 5 C 8603492 = NJW 1989, 2643, 2643; VGH München, Beschluss vom 11.02.2008 – 5 C 08.277, Rn. 2; OVG Koblenz, Urteil vom 26.10.2020 – 10 A 10613/20.OVG = ZD 2021, 446; für die DSRL: Ehmann/Helfrich DSRL, Art. 28, Rn. 11; *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 168 f.

[283] Vgl. zur fehlenden Anordnungsbefugnis *Schmeling*, DuD 2002, 351, 351; ebenso zur fehlenden Anordnungsbefugnis ggü. öffentlichen Stellen: BT-Drs. 11/4306, S. 53.

[284] Anders bereits zur DSRL: VG Darmstadt, Urteil vom 18.11.2010 – 5 K 994/10.DA = MMR 2011, 416, 416.

[285] Zum Petitionseinwand: VG Mainz, Urteil vom 22.07.2020 – 1 K 473/19.MZ, Rn. 23. Ebenso: VG

Aufsichtsbehörde.[286] Dieses Beschwerderecht erwächst gem. Art. 78 Abs. 2 DSGVO nach drei Monaten Untätigkeit der Aufsichtsbehörde zu einem Recht auf einen gerichtlichen Rechtsbehelf gegenüber der Aufsichtsbehörde.[287] Zudem besteht gem. Art. 78 Abs. 1 DSGVO für die betroffene Person ein Recht auf einen gerichtlichen Rechtsbehelf bei einer nach Ansicht der Aufsichtsbehörde unbegründeten oder unzulässigen Beschwerde.[288] Die Frage, ob es sich beim Beschwerderecht aus Art. 77 Abs. 1 DSGVO i.V.m. Art. 78 Abs. 1 DSGVO um ein bloßes Petitionsrecht handelt, wurde mittlerweile durch den EuGH entschieden. Demnach handele es sich bei dem Beschwerdeverfahren gem. Art. 77 Abs. 1 DSGVO um kein petitionsähnliches Verfahren.[289] Die Beschlüsse der Aufsichtsbehörden können auch vollumfänglich gerichtlich überprüft werden.[290] Unabhängig davon stehen der Aufsichtsbehörde mit Art. 58 Abs. 2 DSGVO Abhilfebefugnisse gegenüber dem Verantwortlichen zu.[291] Dabei differenziert die DSGVO nicht zwischen öffentlichen und nicht-öffentlichen Stellen.[292] Einen Anspruch auf eine konkrete Maßnahme hat die betroffene Person zwar nicht,[293] allerdings dürfte das generelle Ziel des Abstellens des Verstoßes ausreichend sein.[294] Konkret im Hinblick auf Behörden ist die Datenschutzaufsicht als spezifische Rechtsaufsichtsbehörde gegenüber diesen ausgestaltet.[295] Dabei handelt sie nicht per Verwaltungsakt, sondern agiert als Rechtsaufsicht per Anweisung.

Ansbach, Urteil vom 08.08.2019 – AN 14 K 19.00272, Rn. 27, 43 ff., die aber keine Verwaltungsaktqualität des Handelns der Aufsichtsbehörde erkennen, vgl. Rn. 21 ff. M.w.N.: Kühling/Buchner/*Bergt*, Art. 77 DS-GVO, Rn. 17.

[286] Zu den engen Ausnahmen: Kühling/Buchner/*Bergt*, Art. 77 DS-GVO, Rn. 18 ff.

[287] Vgl. knapp zur DSRL Kühling/Buchner/*Bergt*, Art. 77 DS-GVO, Rn. 2.

[288] Kritisch, aber offengelassen: OVG Hamburg, Urteil vom 07.10.2019 – 5 Bf 279/17, 22 ff.; Kühling/Buchner/*Bergt*, Art. 78 DS-GVO, Rn. 7.

[289] EuGH, Urteil vom 07.12.2023 – C-26/22, C-64/22 (SCHUFA Holding) = EuZW 2024, 219, Rn. 58.

[290] EuGH, Urteil vom 07.12.2023 – C-26/22, C-64/22 (SCHUFA Holding) = EuZW 2024, 219, Rn. 59 ff.

[291] Diese dürften im Rahmen des regulären Verwaltungsverfahrens als Verwaltungsakt ergehen, vgl. Kühling/Buchner/*Bergt*, Art. 77 DS-GVO, Rn. 26. Vgl. insb. zur Rechtsverbindlichkeit der Verwarnung gem. Art. 58 Abs. 2 lit. b DSGVO Kühling/Buchner/*Bergt*, Art. 78 DS-GVO, Rn. 6; ggü. Behörden allgemein: ebd., Rn. 8.

[292] Vgl. zu den Befugnissen der (Datenschutz-)Aufsichtsbehörde ggü. Behörden *Reimer*, DÖV 2018, 881, 889.

[293] VG Mainz, Beschluss vom 29.08.2019 – 1 L 605/19.MZ, Rn. 5; VG Ansbach, Urteil vom 16.03.2020 – AN 14 K 19.00464, Rn. 19 ff.

[294] Kühling/Buchner/*Bergt*, Art. 77 DS-GVO, Rn. 17; zu den Informationspflichten der Aufsichtsbehörde: ebd., Rn. 23.

[295] Kühling/Buchner/*Bergt*, Art. 78 DS-GVO, Rn. 8; *Voßhoff/Hermerschmidt*, PinG 2016, 56, 59.

Dass sich die Datenschutzaufsichtsbehörden darüber hinaus „grundsätzlich“[296] von normalen Ordnungsbehörden unterscheiden sollen, ist nicht nachvollziehbar. Aufgrund des Fokus auf die Wahrung des Grundrechts auf Schutz personenbezogener Daten gem. Art. 8 Abs. 1 GRCh wird die Datenschutzaufsicht nicht zu einem aliud im Vergleich zu anderen Ordnungsbehörden.[297] Vielmehr dürfte dies für ein Verständnis als Sonderordnungsbehörde sprechen. Näherliegender ist es die Datenschutzaufsichtsbehörden aus der üblichen Fach- und Rechtsaufsichtsordnung[298] herauszulösen.[299] Denn die Ubiquität von Datenverarbeitungen legt die, tatsächlich besondere, völlige Unabhängigkeit der Datenschutzaufsicht gem. Art. 52 DSGVO nahe. Datenschutzaufsichten müssen gegebenenfalls auch gegenüber ihnen potenziell übergeordneten Behörden Anweisung treffen können. Diese Unabhängigkeit der Datenschutzaufsicht führt allerdings nicht zu einer grundsätzlich anderen Bewertung hinsichtlich der inhaltlichen Art ihrer Aufsicht.[300]

Kaum abstreiten lässt sich aber, dass die Datenschutzaufsicht eine atypische Aufsichtsform darstellt.[301] Von dem Fokus auf die Gefahrenvorsorge ausgehend lässt sich das Datenschutzrecht am ehesten noch mit dem Umweltrecht im Sinne eines Risikoverwaltungsrechts[302] vergleichen. Das Risikoverwaltungsrecht ist von einer generellen Unkalkulierbarkeit der Wahrscheinlichkeit der bekannten Szenarien, dem Bestehen noch unbekannter Szenarien und deren Folgen in Gefahrensituationen geprägt.[303] Bei der Informationsgesellschaft, auf die das Datenschutzrecht reagiert, handelt es sich um

---

[296] So: *Tinnefeld/Petri*, MMR 2010, 157, 158.

[297] So a.: *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 205; vgl. zudem *Schmeling*, DuD 2002, 351, 353.

[298] S.: *Schiedermair*, § 48 Selbstkontrollen der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band III - Personal Finanzen Kontrolle Sanktionen Staatliche Einstandspflichten, [2]2013, Rn. 21 ff.

[299] *Schiedermair*, § 48 Selbstkontrollen der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band III - Personal Finanzen Kontrolle Sanktionen Staatliche Einstandspflichten, [2]2013, Rn. 55 ff.; vgl. zur ähnlichen Problematik bei der BNetzA *Ruffert*, § 22 Grundfragen der Wirtschaftsregulierung, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 1 Öffentliches Wirtschaftsrecht, [4]2019, Rn. 30 f.

[300] *Lewinski/Herrmann*, ZD 2016, 467, 472.

[301] Vgl. a. *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 203 mit Hinweis auf die Ministerialfreiheit der Datenschutzaufsichten.

[302] S.: *Schulze-Fielitz*, § 12 Grundmodi der Aufgabenwahrnehmung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band I - Methoden Aufgaben Organisation, [2]2012, Rn. 31; inwiefern hierbei aber wiederum ein „plus“ gegenüber der Gefahrenabwehr und der Wirtschaftsaufsicht vorliegt: ebd., Rn. 33. Zum Begriff: *Sommermann*, § 86 Prinzipien des Verwaltungsrechts, in: Bogdandy/Cassese/Huber (Hrsg.), Band V Verwaltungsrecht in Europa: Grundzüge, 2014, Rn. 46 f.

[303] Vgl. *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 279 ff.

eine Erscheinungsform der Risikogesellschaft.[304] Auch die neueren Wirtschaftsgesetze verlangen allerdings teilweise, ähnlich dem Vorfeldschutz des Datenschutzrechts, eine Gefahrenvorsorge.[305] Damit soll bereits ein Bereich vor der Gefahrenschwelle abgebildet werden, um Fälle geringer Eintrittswahrscheinlichkeit, zeitlich und räumlich entferntere Fälle sowie summierende Fälle erfassen zu können.[306] Allgemein findet sich im Gefahrenabwehrrecht ein zunehmender Fokus auf Prävention und Vorsorge.[307] Auch dieser Aspekt ist also kein Alleinstellungsmerkmal das Datenschutzrechts.[308]

3. Fazit

Insgesamt sprechen keine gewichtigen Gründe dagegen die Datenschutzaufsicht als Sonderordnungsbehörde zu erachten und im Rahmen dessen auch das Datenschutzrecht, jedenfalls in seiner aufsichtsbehördlichen Dimension, als besonderes Ordnungsrecht zu begreifen.[309] So hatte das BVerwG für § 38 Abs. 5 BDSG a.F. bereits festgestellt, dass die Norm keinen Ansatz dafür biete, einen Rückgriff auf die allgemeinen Grundsätze der Störerauswahl auszuschließen.[310] Neben Konsequenzen für die Störerauswahl bei mehreren Verantwortlichen ist dabei der Rückgriff auf Störer bzw. Adressaten nach dem allgemeinen Polizei- und Ordnungsrecht denkbar.

---

[304] *Hoffmann-Riem*, Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer/Micklitz/Tonner (Hrsg.), Law and diffuse Interests in the European Legal Order: Liber amicorum Norbert Reich, 1997, 782.

[305] Ausführlicher: *Ehlers*, § 1 Wirtschaft als Gegenstand des öffentlichen Rechts, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 1 Öffentliches Wirtschaftsrecht, [4]2019, Rn. 22; *Wißmann*, § 14 Grundmodi der Aufgabenwahrnehmung, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, [3]2022, Rn. 98; *Lennartz*, RdV 1990, 25, 28.

[306] *Ossenbühl*, NVwZ 1986, 161, 163 f.

[307] *Wißmann*, § 14 Grundmodi der Aufgabenwahrnehmung, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, [3]2022, Rn. 96 f.

[308] Siehe etwa die Vergleiche mit dem Umweltrecht bei: *Mutius*, Neuorganisation des staatlichen Datenschutzes in Schleswig-Holstein, in: Bäumler/Mutius (Hrsg.), Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts, 1999, 94.

[309] Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 98, 101; Paal/Pauly/*Körffer*, Art. 58 DSGVO, Rn. 31. Unproblematisch scheinbar: BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 30. Bereits 1979: *Bull*, NJW[32] (1979), 1177, 1180. Ebenso: *Mutius*, Neuorganisation des staatlichen Datenschutzes in Schleswig-Holstein, in: Bäumler/Mutius (Hrsg.), Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts, 1999, 94 f., 101; *Schmeling*, DuD 2002, 351, 352; *Roßnagel*, MMR 2005, 71, 74. Wohl a.: *Albers*, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, [2]2012, Rn. 103. Ablehnend: *Spiecker gen. Döhmann*, JZ 2010, 787, 788.

[310] BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 29.

II. Adressaten im besonderen Gefahrenabwehrrecht

Ausgehend davon, dass die aufsichtsbehördlichen Maßnahmen der DSGVO größtenteils ordnungsrechtlicher Natur sind,[311] ist also ein Rückgriff auf die allgemeinen polizei- und ordnungsrechtlichen Grundsätze und Regelungen möglich.[312] Üblicherweise beinhaltet besonderes Gefahrenabwehrrecht eigene Normen für die Adressaten von aufsichtsbehördlichen Maßnahmen, also für die Pflichtigen,[313] Verantwortlichen oder Störer.[314] Ebenso kann aber auch ein Verweis auf die Adressaten des allgemeinen Gefahrenabwehrrechts erfolgen.[315] Dies erfolgt etwa regelmäßig in den Landesbauordnungen.[316] Benennen dort die Eingriffsbefugnisse keine Adressaten und werden solche auch nicht anderweitig in der LBauO benannt,[317] greifen die LBauO auf das allgemeine Polizei- und Ordnungsrecht zurück.[318] Verhält sich besonderes Gefahrenabwehrrecht überhaupt nicht zu dem Adressaten einer Maßnahme – weder allgemein noch in einer konkreten Eingriffsbefugnis – ist ein Rückgriff auf die Adressaten des allgemeinen Gefahrenabwehrrecht denkbar, sofern sich der Adressat nicht anderweitig bestimmen lässt.[319] Zu diesen Adressaten gehört neben dem Zweckveranlasser als Sonderform des Verhaltensstörers auch die Inanspruchnahme nicht verantwortlicher Personen.

---

[311] Dazu: Kapitel 5 K. I. Aufsichtsbehördliche Maßnahmen als Gefahrenabwehrrecht.

[312] *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 20, 22; *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 183. Allgemein: *Thiel*, Polizei- und Ordnungsrecht, [3]2022, § 6 Rn. 12. Vgl. für das Bauordnungsrecht *Kaiser*, § 41 Bauordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, [4]2020, Rn. 12.

[313] Dabei scheint der Begriff des Pflichtigen neutraler, da teilweise auch eine Inanspruchnahme des Nichtverantwortlichen in Frage kommt, vgl. § 7 POG RLP.

[314] Vgl. etwa §§ 54 ff. LBauO RLP.

[315] Vgl. § 59 Abs. 2 LBauO RLP i.V.m. § 7 POG RLP.

[316] *Kaiser*, § 41 Bauordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, [4]2020, Rn. 145.

[317] Wie etwa §§ 54 ff. LBauO RLP.

[318] Strittig ist, ob diese Adressatennormen parallel gelten können, die LBauO also nicht lex specialis ist. Dafür scheinbar: OVG Lüneburg, Beschluss vom 19.12.2018 – 1 ME 155/18 = NVwZ 2019, 334, 335; ablehnend: *Beckermann*, DÖV 2020, 144, 148.

[319] Vgl. *Beckermann*, DÖV 2020, 144, 145 zu diesem Automatismus.

Davor ist allerdings zu klären, ob die jeweilige spezialgesetzliche Ermächtigungsgrundlage – für die Aufsichtsbehörden Art. 58 DSGVO – die Eingriffsvoraussetzungen abschließend[320] regelt.[321] Denn dann hat eine spezialgesetzliche Ermächtigungsgrundlage nicht nur Anwendungsvorrang, sie entfaltet auch eine Sperrwirkung gegenüber einer ordnungsrechtlichen Generalklausel.[322] Dies gilt auch dann, wenn nur einzelne Tatbestandsmerkmale einer Norm im konkreten Anwendungsfall nicht erfüllt sind, allerdings deren Anwendung insgesamt möglich ist.[323] Die Sperrwirkung gilt aber nur insoweit die spezialgesetzliche Ermächtigungsgrundlage alle Merkmale einer Eingriffsbefugnis abbildet,[324] insbesondere also auch die Adressaten benennt oder wenigstens erkennen lässt.[325] Denkbar wäre demnach eine Norm, die zwar die Tatbestandsmerkmale eines Eingriffs regelt,[326] zu den Adressaten aber schweigt.[327] Um festzustellen, ob ein Gesetz die Eingriffsvoraussetzungen und damit etwa auch Adressaten abschließend regelt, ist zweistufig vorzugehen. Zunächst ist festzustellen, ob die Eingriffsbefugnis selbst Adressaten benennt. Danach ist festzustellen, ob im selben Gesetz allgemeine

[320] *Thiel*, Polizei- und Ordnungsrecht, [5]2022, § 6 Rn. 13 f.

[321] *Wegricht*, Das Verhältnis von Eingriffsermächtigungen des Bundes-Immissionsschutzgesetzes zur polizeilichen Generalklausel, 2008, 112 schlägt vor, dies grundsätzlich im Hinblick auf die einzelne Norm zu prüfen.

[322] *Graulich*, E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 271 ff.; *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 21, 39; *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 183; *Kingreen/Poscher*, Polizei- und Ordnungsrecht, [12]2022, § 5 Rn. 11; *Wegricht*, Das Verhältnis von Eingriffsermächtigungen des Bundes-Immissionsschutzgesetzes zur polizeilichen Generalklausel, 2008, 113; § 9 Abs. 2 POG RLP.

[323] *Kingreen/Poscher*, Polizei- und Ordnungsrecht, [12]2022, § 5 Rn. 14.

[324] *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 182.

[325] *Kingreen/Poscher*, Polizei- und Ordnungsrecht, [12]2022, § 11 Rn. 2; vgl. zum Rückgriff auf die Adressaten ebd., § 2 Rn. 52; ebd., § 19 Rn. 5. Vgl. zum Verantwortlichen *Wittner*, Verantwortlichkeit in komplexen Daten-Ökosystemen, 2022, 281 ff.

[326] Etwa die Gefahr. So spricht Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 7 davon, dass die Befugnisnormen der datenschutzrechtlichen Aufsichtsbehörden gem. Art. 58 DSGVO diejenigen der allgemeinen Polizei- und Ordnungsbehörden verdrängen.

[327] *Beckermann*, DÖV 2020, 144, 145 erkennt ein besonderes Bedürfnis für diese Ergänzung von Fachgesetzen.

Regelungen zu den Adressaten getroffen werden und erst dann wäre auf die allgemeinen ordnungsrechtlichen Adressaten zurückzugreifen.[328]

III. Adressaten in der DSGVO

Neben der individuellen Festlegung von Adressaten in den konkreten Befugnissen in Art. 58 DSGVO findet sich keine allgemeine Festlegung der Adressaten für die Befugnisse der Aufsichtsbehörden im maßgeblichen Kapitel VI, Abschnitt 2[329]. Art. 55 DSGVO definiert nur den materiellen[330] und räumlichen Zuständigkeitsbereich der Aufsichtsbehörden. Dabei rekurriert die Norm indirekt, in Abs. 2 und 3, auf den sachlichen Anwendungsbereich der DSGVO, also die Verarbeitung. Dieser Bezug zur Verarbeitung ist hinsichtlich der Adressaten allerdings nicht weiterführend.[331] So muss bei gemeinsam Verantwortlichen nicht jeder Verantwortliche Zugang zu den Daten haben.[332] Ebenso muss auch der Verantwortliche bei einer Auftragsverarbeitung nicht Zugang zu den Daten haben.[333]

Eine Norm, die explizit den oder die Adressaten der Verordnung festlegt, findet sich auch in der DSGVO insgesamt nicht. Als potenzielle Adressaten erwähnt Art. 58 DSGVO in den jeweiligen Eingriffsbefugnissen unter anderem den Verantwortlichen, den Auftragsverarbeiter sowie den Vertreter des Verantwortlichen oder des Auftragsverarbeiters.[334] Auffällig ist dabei, dass Art. 58 DSGVO grundsätzlich entweder direkt oder indirekt durch Verweis auf eine andere[335] Norm, einen Adressaten der Eingriffsbefugnisse nennt, so die bereits genannten oder in Art. 58 Abs. 2 lit. h DSGVO

[328] Vgl. *Graulich*, E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Bäcker/Denninger/Graulich (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, [7]2021, Rn. 271 ff.; *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 180. Vgl. allgemein *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 25, 84 zum Rückgriff auf Generalklauseln.

[329] „Unabhängige Aufsichtsbehörden - Zuständigkeit, Aufgaben und Befugnisse".

[330] Also Aufgaben und Befugnisse.

[331] Anders: Taeger/Gabel/*Grittmann*, Art. 58 DSGVO, Rn. 29.

[332] EuGH, Urteil vom 10.07.2018 – C-25/17 (Jehovan todistajat) = ZD 2018, 469, Rn. 69.

[333] Vgl. Simitis/Hornung/Spiecker/*Petri*, Art. 28 DSGVO, Rn. 78.

[334] Abs. 1 lit. a, c (via Art. 42 Abs. 7) d, e, f - Abs. 2 lit. a, b, c, d, e, g (via Art. 16 - 18), i (via Art. 83), j (via Art. 44 ff.) - Abs. 3 lit. a, c (via Art. 36 Abs. 5), f (via Art. 42), h (via Art. 46), i (via Art. 46).

[335] Vgl. für Art. 83 DSGVO Kühling/Buchner/*Bergt*, Art. 83 DS-GVO, Rn. 22.

die Zertifizierungsstellen.[336] Eine allgemeine Festlegung der Adressaten scheint also hinfällig.[337] Eine Abweichung von dieser Vorgehensweise stellen aber die Eingriffsbefugnisse in Art. 58 Abs. 1 lit. b sowie Art. 58 Abs. 2 lit. f[338] DSGVO dar.[339]

Dass die Untersuchungsbefugnis aus Art. 58 Abs. 1 lit. b DSGVO keinen Adressaten erkennen lässt, ist allerdings unproblematisch. Denn die Untersuchungsbefugnisse in Art. 58 Abs. 1 DSGVO sind auch Mittel dazu, eine Verantwortlichkeit überhaupt festzustellen. Dies gilt erst recht für Datenschutzüberprüfungen, die dazu dienen, die tatsächlichen Umstände einer Verarbeitung festzustellen. Vorteilhaft kann eine solche adressatenoffene Untersuchungsbefugnis etwa im Hinblick auf die Auskunftspflicht ehemaliger Mitarbeiter eines Verantwortlichen sein, da diese nicht mehr organisatorischer Teil des Verantwortlichen sind.[340]

Bei der Abhilfebefugnis des Art. 58 Abs. 2 lit. f DSGVO könnte sich der Verantwortliche als Normadressat über den Bezug zur Verarbeitung ergeben.[341] Der Verantwortliche bestimmt sich aber nicht notwendigerweise durch die Durchführung der Verarbeitung,[342] sondern anhand der Entscheidung über deren Zwecke und Mittel. Die Erwähnung der Verarbeitung allein deutet also noch nicht auf den Verantwortlichen als Adressaten hin. Der Begriff der Verarbeitung ist nach Art. 2 Abs. 1 DSGVO zwar elementare Voraussetzung für den sachlichen Anwendungsbereich der DSGVO.[343] Eine Norm, die den persönlichen Anwendungsbereich der DSGVO festlegt, vergleichbar zum sachlichen Anwendungsbereich nach Art. 2 DSGVO sowie dem räumlichen Anwendungsbereich nach Art. 3 DSGVO, existiert aber gerade nicht.[344] Somit wird

---

[336] So kritisiert Sydow/Marsch/*Ziebarth*, Art. 58 DS-GVO, Rn. 10, dass der Vertreter ausdrücklich nur bei Art. 58 Abs. 1 lit. a DSGVO genannt wird, trotz der Feststellungen in ErwGr 80 DSGVO.

[337] Vgl. Ehmann/Selmayr/*Selmayr*, Art. 58 DS-GVO, Rn. 8.

[338] Hier wird vielfach einfach der Verantwortliche als Adressat unterstellt: Ehmann/Selmayr/*Selmayr*, Art. 58 DS-GVO, Rn. 24.

[339] Auch die englische oder französische Sprachfassung lassen keinen Adressaten erkennen.

[340] *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 171.

[341] A. ErwGr 129 S. 2 DSGVO nimmt keine Stellung zum Adressaten.

[342] Wie ausgehend vom Wortlaut im BDSG a.F.

[343] So leitet *Lewinski/Herrmann*, PinG 2017, 209, 210 den Adressaten bzw. die Nicht-Adressaten über den Anwendungsbereich her (mit Verweis auf § 40 BDSG: „ [...] überwachen [...] die Anwendung der Vorschriften über den Datenschutz."). Ebenso: Kühling/Buchner/*Boehm*, Art. 58 DS-GVO, Rn. 26; Simitis/Hornung/Spiecker/*Polenz*, Art. 58 DSGVO, Rn. 41.

[344] *Mantz/Marosi*, § 3 Vorgaben der Datenschutz-Grundverordnung, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht: Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, 2019, Rn. 18. Dieser Aspekt wird eben gerade nicht geregelt, folglich findet hier prima facie keine Vollharmonisierung statt, vgl. *Gsell/Schellhase*, JZ 2009, 20, 25. Bei Art. 3 VRRL (RL 2011/83/EU) etwa wird über den Geltungsbereich, aufgrund der expliziten Erwähnung des Unternehmers, der Normadressat erkennbar.

auch nicht der Verantwortliche als allgemeiner Adressat der DSGVO festgelegt. Die Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO besitzt für sich genommen noch keine Aussagekraft hinsichtlich seiner Bedeutung. Diese erwächst erst aus der Bezugnahme anderer Normen auf den definierten Begriff. Im Gegensatz zur Verarbeitung taucht der Begriff des Verantwortlichen in Art. 58 Abs. 2 lit. f DSGVO gar nicht auf. Abseits eines irgendwie gearteten Bezugs zum Verantwortlichen scheint ein Rückgriff auf den Verantwortlichen, nur anhand der Definition, also willkürlich.[345] Dies gilt umso mehr, als das Verbot der Verarbeitung die eingriffsintensivste Maßnahme der Aufsichtsbehörde darstellt.[346] Daher verbietet sich auch eine Herleitung des Verantwortlichen als Adressaten anhand der übrigen Befugnisse der Aufsichtsbehörde.[347] Man könnte unter dem Aspekt der Intensität des Verbots der Verarbeitung nun zweierlei annehmen. Zum einen, dass ein Verbot nur gegenüber dem Verantwortlichen als überwiegendem Adressaten der DSGVO erfolgen können sollte. Ebenso kann man aber auch annehmen, dass ein Verbot wegen der Effektivität der Gefahrenabwehr bzw. dem effet utile schnellstmöglich ohne größere Rücksicht auf die Auswahl des Adressaten durchgesetzt werden sollte. Dabei muss der Verantwortliche, etwa bei einer Auftragsverarbeitung oder Konzernstrukturen, nicht notwendigerweise der ideale Ansatzpunkt sein. Ebenso könnte also auch der Auftragsverarbeiter oder der Vertreter von Art. 58 Abs. 2 lit. f DSGVO erfasst sein. Weder die Systematik der Befugnisse noch die Intensität der Maßnahme lassen also einen sicheren Rückschluss auf den Verantwortlichen als Adressaten zu.[348]

Systematisch wäre auch ein Rückgriff auf Art. 5 Abs. 2 DSGVO denkbar. Nach der sogenannten Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO ist der Verantwortliche verantwortlich für die Einhaltung des Abs. 1 und muss dies auch nachweisen können. Sofern aber Art. 5 Abs. 2 DSGVO allgemein den Verantwortlichen als Adressat der DSGVO normiert, wäre die Nennung des Verantwortlichen in den individuellen Befugnissen in Art. 58 DSGVO wiederum überflüssig. Notwendig wäre dann nur die Benennung weiterer Adressaten, etwa des Auftragsverarbeiters. Zudem verpflichtet Art. 5

[345] Zu Art. 3 Abs. 2 DSGVO und der Zuständigkeit der Aufsichtsbehörde vergleichbare Erwägungen zum Vertreter bei: Simitis/Hornung/Spiecker/*Hornung*, Art. 3 DSGVO, Rn. 65. A. die Art. 29-Datenschutzgruppe will für die DSRL den Verantwortlichen global nur für die Pflichten angesprochen wissen: *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", 16.02.2010, 5.

[346] Zu potenziellen Beweggründen für eine Regelungstechnik mit Generalklausel: *Gsell/Schellhase*, JZ 2009, 20, 24.

[347] So: Auernhammer/*Lewinski*, Art. 58 DSGVO, Rn. 6.

[348] So erwägt Kühling/Buchner/*Bergt*, Art. 83 DS-GVO, Rn. 23 a. die Bebußung Dritter aufgrund der Missachtung einer Anordnung nach Art. 58 Abs. 2 DSGVO.

Abs. 2 DSGVO den Verantwortlichen nur auf Abs. 1 der Norm. Damit ist zwar auch die Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 lit. a DSGVO erfasst, diese wiederum bezieht sich aber erkennbar auf Art. 6 DSGVO.[349]

Darüber hinaus sind in der DSGVO keine weiteren Andeutungen eines allgemeinen Adressaten ersichtlich.[350] Weder Wortlaut noch Systematik führen daher bei Art. 58 Abs. 2 lit. f DSGVO zu einem klaren Ergebnis. Die historische Auslegung schließlich findet im Unionsrecht, ohne Anklang im Gesetzestext, kaum Berücksichtigung.[351] Insgesamt lässt sich also im Rahmen einer Auslegung von Art. 58 Abs. 2 lit. f DSGVO kein eindeutiger Anhaltspunkt für den Verantwortlichen als Normadressaten erkennen.

IV. Systematische Konflikte in der DSGVO

Eine Überschneidung mit dem Konzept des gemeinsam Verantwortlichen ist aufgrund der Inanspruchnahme weiterer Adressaten für Art. 58 Abs. 2 lit. f DSGVO nicht ersichtlich. Zwar wird der gemeinsam Verantwortliche in der Rechtsprechung des EuGH weit ausgelegt. Die Verantwortlichkeit ist allerdings durch die Vorgänge begrenzt, an denen der gemeinsam Verantwortliche aufgrund seiner Entscheidungsbeiträge beteiligt ist.[352] Der EuGH hatte in dem Urteil zu der Rechtssache Fashion ID explizit darauf hingewiesen, dass gegenüber der eigenen Verantwortlichkeit vor- oder nachgelagerten Vorgängen eine zivilrechtliche Haftung im mitgliedstaatlichen Recht vorgesehen werden kann.[353] Es ist nicht ersichtlich, warum eine solche weitergehende Haftung nicht auch nach öffentlichem Recht eingeschränkt auf ein Verbot bzw. eine Beschränkung der Verarbeitung bestehen könnte. Insofern könnte durch einen Rückgriff auf den Nichtstörer[354] eine Lücke in der Durchsetzung geschlossen werden, wenn eine gemeinsame Verantwortlichkeit des Adressaten nicht begründet werden kann, dieser aber dennoch die Verarbeitung unmittelbar beeinflussen kann.

Sofern ein Rückgriff auf den Nichtstörer nur in diesem begrenzten Rahmen erfolgen würde, wäre auch kein Verstoß gegen den freien Datenverkehr gem. Art. 1 Abs. 3

---

[349] Zur Frage, ob Art. 5 Abs. 2 DSGVO eine globale Verpflichtung zur Rechtmäßigkeit enthält: Kapitel 1 A. II. 1. Der Verantwortliche im Kontext seiner Pflichten und seiner Verantwortung.

[350] Zur Problematik eines negativ regelnden Charakters und der abschließenden Regelung: *Gsell/Schellhase*, JZ 2009, 20, 22 f., 25.

[351] Groeben, von der/Schwarze/*Gaitanides*, Art. 19 EUV, Rn. 47; Ehmann/Selmayr/*Selmayr/Ehmann*, Einleitung, Rn. 104; unklar: EuGH, Urteil vom 01.10.2019 – C-673/17 (Planet 49) = EuZW 2019, 916, Rn. 48.

[352] Dazu: Kapitel 4.

[353] Dazu: Kapitel 5 J. II. Rechtsprechung des EuGH. EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74.

[354] Etwa: § 7 POG RLP.

DSGVO ersichtlich. Mangels Verantwortlichkeit der Nichtstörer könnte der freie Datenverkehr streng genommen auch gar nicht behindert werden. Denn solche Nichtstörer erbringen regelmäßig nur Hilfsleistungen gegenüber den Verantwortlichen, übermitteln aber nicht selbst personenbezogene Daten.

Bei der Einschränkung oder dem Verbot einer Verarbeitung nach Art. 58 Abs. 2 lit. f DSGVO gegenüber dem Nichtstörer, die sowohl vorübergehend als auch endgültig möglich ist, ginge es nicht darum den Nichtstörer zu sanktionieren, sondern dem Verstoß des eigentlich Verantwortlichen entgegenzuwirken. Dabei wären Maßnahmen, sofern erfolgversprechend, zunächst gegen den eigentlich Verantwortlichen zu richten. Mildere Maßnahmen gegen einen Nichtstörer aus dem Katalog des Art. 58 Abs. 2 lit. f DSGVO sind nicht ersichtlich. Dieser dürfte aber jenseits der Ermöglichung einer Verarbeitung regelmäßig auch keine weitere Einflussmöglichkeit auf die Verarbeitung haben. Im Rahmen des Verhältnismäßigkeitsgrundsatzes wäre daher immer zunächst eine nur vorübergehende Einschränkung der Verarbeitung zu erwägen. Die Vorgabe, dass eine Inanspruchnahme von Nichtstörern nur solange möglich ist, wie die Abwehr der Gefahr nicht auf andere Weise möglich ist,[355] würde dafür sorgen, dass, sobald möglich, der Verantwortliche selbst verpflichtet wird. Eine vorübergehende Einschränkung oder ein Verbot einer Verarbeitung erscheint dabei als deutlich milderes Mittel gegenüber den Konsequenzen eines weiten Verständnisses der gemeinsamen Verantwortlichkeit etwa hinsichtlich der möglichen Folgen von hohen Schadensersatzansprüchen oder Geldbußen. Auch die Haftungsprivilegierungen in Art. 4 - 6 des DSA sehen die Möglichkeit für mitgliedstaatliches Recht vor, dass eine Verwaltungsbehörde oder ein Gericht verlangen kann, dass eine Rechtsverletzung abgestellt oder verhindert wird. Dies gilt selbst für die sehr weitreichende Privilegierung der reinen Durchleitung. Vergleichbare Ansätze sind dem Unionsrecht also nicht fremd.

Auch die Bedeutung des Grundrechts auf Datenschutz aus Art. 8 GRCh sowie des effet utile[356] aus Art. 4 Abs. 3 EUV sprechen für ein offenes Verständnis der Adressaten in Art. 58 Abs. 2 lit. f DSGVO. Verarbeitungsverstößen, die die Dringlichkeitsstufe von Art. 58 Abs. 2 lit. f DSGVO erreichen, muss schnellstmöglich Einhalt geboten werden können. Sollte eine Aufsichtsbehörde fälschlicherweise einen Akteur mit einer Maßnahme nach Art. 58 Abs. 2 lit. f DSGVO belegen, bestünden neben dem Rechtsweg nach Art. 78 Abs. 1 DSGVO auch Amtshaftungsansprüche. Daneben könnte an die Inanspruchnahme von Nichtstörern auch eine Schadensersatzpflicht geknüpft werden.

[355] Vgl. § 7 Abs. 2 POG RLP.

[356] Groeben, von der/Schwarze/*Gaitanides*, Art. 19 EUV, Rn. 45. Der effet utile findet sich auch eingeschränkt in Art. 84 Abs. 1 DSGVO wieder. Vgl. zu Art. 24 DSRL *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, 170.

Eine Kostentragungspflicht oder ein Entschädigungsanspruch aufgrund der Maßnahme ließe sich gesondert bzw. allgemein verwaltungsrechtlich regeln.[357] Denkbar wäre insofern auch ein zivilrechtlicher Regress des Nichtstörers gegen den Verantwortlichen. Problematisch wäre hierbei, dass der Nichtstörer das Insolvenzrisiko des Verantwortlichen tragen würde. Alternativ könnte der Staat Regress aufgrund eines Entschädigungsanspruchs des Nichtstörers beim Verantwortlichen nehmen.

V. Materiell-rechtliche Pflichtigkeit des Verantwortlichen

Problematisch erscheint ein solch weites Verständnis des Adressaten in Art. 58 Abs. 2 lit. f DSGVO allerdings im Hinblick auf die materiell-rechtliche Pflichtigkeit des Verantwortlichen.[358] Geht man davon aus, dass Art. 58 Abs. 2 lit. f DSGVO auch Adressaten, die nicht Verantwortliche sind, erfasst, würden materiell-rechtliche Pflichtigkeit und aufsichtsbehördlicher Zugriff auseinanderfallen. Pflichten des Verantwortlichen bestehen sowohl zugunsten der betroffenen Personen als auch zugunsten der Aufsichtsbehörde. Pflichten des Nichtstörers bestehen allerdings gerade nicht, da sich seine Inanspruchnahme darauf stützt, dass Maßnahmen der Aufsichtsbehörde gegenüber dem eigentlich Verantwortlichen nicht rechtzeitig möglich sind oder keinen Erfolg versprechen. Somit könnte der Nichtstörer im Wege der Durchsetzung der Pflichten durch die Aufsichtsbehörde in Anspruch genommen werden, im Wege der Durchsetzung durch die betroffene Person hingegen nicht.[359] Verstünde man die betroffene Person und die Aufsichtsbehörde als zwei voneinander unabhängige Akteure zur Durchsetzung der DSGVO wäre dies unproblematisch. Da die betroffene Person allerdings gem. Art. 77 DSGVO eine Beschwerde über den Verantwortlichen auch bei der Aufsichtsbehörde erheben kann, handelt es sich hier aber eben nicht um zwei völlig unabhängige Durchsetzungsvektoren.[360] Die betroffene Person könnte bei einem offenen Verständnis des Adressaten in Art. 58 Abs. 2 lit. f DSGVO über die Aufsichtsbehörde

[357] *Pünder*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [4]2021, Rn. 353 ff.; *Würtenberger*, § 69 Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, [3]2013, Rn. 276 ff.; *Kingreen/Poscher*, Polizei- und Ordnungsrecht, [12]2022, § 25 Rn. 19.

[358] Vgl. BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 23: „Die personale Reichweite der Eingriffsbefugnis folgt hier der materiellrechtlichen Pflichtigkeit."

[359] Denkbar wäre dies allerdings im Rahmen eines gerichtlichen Verfahrens.

[360] Vgl. zur DSRL EuGH, Urteil vom 13.05.2014 – C-131/12 (Google Spain) = NVwZ 2014, 857, Rn. 77.

indirekt Adressaten erreichen, die sie über die direkte Ausübung der Betroffenenrechte nicht erreichen könnte. Diese Inkohärenz ist nicht unproblematisch.

Allerdings bestehen nicht alle Pflichten des Verantwortlichen sowohl zugunsten der betroffenen Person als auch zugunsten der Aufsichtsbehörde. Es besteht also nicht notwendigerweise ein Dualismus der Pflichten des Verantwortlichen. So dient etwa das Verarbeitungsverzeichnis nach Art. 30 Abs. 4 DSGVO nicht der Durchsetzung der Betroffenenrechte, sondern den Untersuchungsbefugnissen der Aufsichtsbehörde. Während die betroffene Person möglichst einfachen Zugriff auf den Verantwortlichen zwecks der Durchsetzung ihrer Rechte haben soll, etwa anhand von Art. 26 Abs. 3 DSGVO und Art. 82 Abs. 4 DSGVO, bestehen für die Aufsichtsbehörden keine vergleichbaren Erleichterungen.[361] Andererseits hat die Aufsichtsbehörde mit Art. 58 Abs. 2 DSGVO Untersuchungsbefugnisse, die die Erleichterungen des Art. 26 Abs. 3 DSGVO kompensieren können. Speziell für die Einschränkung oder das Verbot einer Verarbeitung findet sich kein spiegelbildliches Betroffenenrecht. So findet der Anspruch auf Löschung der Daten gem. Art. 17 DSGVO, ebenso wie der Anspruch auf Einschränkung der Verarbeitung gem. Art. 18 DSGVO seine Entsprechung in Art. 58 Abs. 2 lit. g DSGVO. Im Umkehrschluss handelt es sich bei Art. 58 Abs. 2 lit. f DSGVO nicht um die Einschränkung oder das Verbot einer einzelnen Verarbeitung, sondern Verbote oder Einschränkungen weitreichenderer Art.[362] Voraussetzung für eine so intensive Maßnahme wäre im Rahmen des Verhältnismäßigkeitsgrundsatzes ein erheblicher Verstoß des eigentlich Verantwortlichen. Ein weites Verständnis des Adressaten in Art. 58 Abs. 2 lit. f DSGVO erscheint im Hinblick auf den Ausnahmecharakter dieser Abhilfebefugnis, sowie die Verpflichtung der Aufsichtsbehörde auf den Verhältnismäßigkeitsgrundsatz,[363] auch bezüglich der Pflichtigenauswahl, ausnahmsweise möglich.[364] Dabei muss aber der Kreis von potenziellen Nichtstörern eingegrenzt werden. So könnte etwa bei äußerst geringen Entscheidungsbeiträgen statt einer gemeinsamen Verantwortlichkeit eine Inanspruchnahme von Zweckveranlassern oder Nichtstörern

[361] So gibt es etwa keine Gesamtschuld bei der Geldbuße nach Art. 83 DSGVO.

[362] Denkbar wären hier identische Verarbeitungen über viele betroffene Personen hinweg, ebenso abstrakt rechtswidrige Verarbeitungen, die auch im Einzelfall nicht rechtmäßig durchgeführt werden könnten. In jedem Fall würde es um Szenarien gehen, die quantitativ risikobehafteter wären als einzelne Verarbeitungen. Vgl. zum Unterlassungsanspruch im deutschen Zivilrecht *Hense*, DSB[44] (2020), 236, 237. Letzteres kann man als Wahrnehmung des mitgliedstaatlichen Spielraums aus EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74 verstehen.

[363] Vgl. zu diesem Grundsatz auch die Notwendigkeit eines gestuften Vorgehens im BDSG a.F. BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 18. Zu den grundrechtlichen Anforderungen an verwaltungsrechtliche Sanktionen: Kühling/Buchner/*Bergt*, Art. 84 DS-GVO, Rn. 5.

[364] Vgl. zur Ermessensausübung hinsichtlich potenzieller Adressaten BVerwG, Urteil vom 11.09.2019 – 6 C 15.18 = ZD 2020, 264, Rn. 29.

erwogen werden.[365] Ebenso könnten gemeinsam Verantwortliche für nicht mehr von ihnen verantwortete nachgelagerte Verarbeitungsvorgänge als Nichtstörer in Anspruch genommen werden. Allgemein wäre eine Inanspruchnahme von Nichtstörern dann denkbar, wenn diese die Verarbeitung ermöglichen oder notwendige Leistungen hierzu beisteuern. Keinesfalls sollte die Inanspruchnahme von Nichtstörern auf weit von der Verarbeitung entfernte Akteure wie Internet-Provider oder Stromversorger erstreckt werden.[366]

Ein Auseinanderfallen von materiellrechtlicher Haftung gegenüber Privaten und der Inanspruchnahme durch Verwaltungsbehörden (und Gerichte) findet sich auch in den Privilegierungen von Art. 4 - 6 DSA.[367] So sehen Art. 4 Abs. 3, Art. 5 Abs. 2 und Art. 6 Abs. 4 DSA vor, dass ungeachtet der jeweiligen Privilegierung „[...] eine Justiz- oder eine Verwaltungsbehörde nach dem Rechtssystem eines Mitgliedstaats vom Diensteanbieter verlang[en kann], eine Zuwiderhandlung abzustellen oder zu verhindern." Auch der DSA sieht also keinen Gleichlauf der Maßnahmen zwischen Privaten und Verwaltungsbehörde vor.

Insgesamt muss also die Durchsetzung der DSGVO durch die betroffene Person nicht der Durchsetzung durch die Aufsichtsbehörden entsprechen. Man sollte hier von einem Ergänzungs- und weniger einem deckungsgleichen Verhältnis der Durchsetzungsmöglichkeiten ausgehen.[368]

VI. Adressaten in der DSRL

Hilfreich im Hinblick auf das Verständnis des Adressaten in Art. 58 Abs. 2 lit. f DSGVO ist, trotz der konzeptionellen Überarbeitung der Befugnisse der Aufsichtsbehörde in Art. 58 DSGVO, möglicherweise auch ein Blick auf die DSRL. So wurde in der Begründung[369] zum geänderten Vorschlag der Kommission der für die Verarbeitung Verantwortliche – und nur dieser – ausdrücklich als Adressat für die Einwirkungsbefugnisse der Aufsichtsbehörde nach Art. 28 Abs. 3 DSRL genannt.[370] Im geänderten

[365] Problematisch wäre hier allerdings der Widerspruch zur bisherigen Rechtsprechung des EuGH.

[366] Vgl. zur Reichweite der gemeinsamen Verantwortlichkeit EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 74.

[367] Vgl. noch zur e-Commerce-RL *Sartor*, MJ[21] (2014), 564, 571.

[368] Vgl. Dammann/Simitis DSRL/*Simitis*, Einleitung, Rn. 37; Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 37.

[369] Entsprechende Materialien für die DSGVO gibt es nicht.

[370] BT-Drs. 12/8329, S. 42.

Vorschlag[371] selbst wurde dies, wie auch in der verabschiedeten Version, bis auf die Befugnis zur Verwarnung, nicht deutlich.[372] Ähnliches galt für die Untersuchungsbefugnisse nach Art. 28 Abs. 3 DSRL.[373] Bei den Untersuchungsbefugnissen fand der für die Verarbeitung Verantwortliche im Normtext sogar überhaupt keine Erwähnung. Trotz der Eindeutigkeit der Gesetzesmaterialien sind diese Erwägungen allerdings kaum weiterführend, denn die Dokumente des Gesetzgebungsprozesses finden bei der Auslegung von Unionsrecht kaum Beachtung, sofern sie nicht Anklang im Gesetzestext finden.[374]

Grundsätzlich war der für die Verarbeitung Verantwortliche Adressat der DSRL. Art. 6 Abs. 2 DSRL benannte den für die Verarbeitung Verantwortlichen explizit, ebenso Art. 10, 11, 12, 14, 17, 18 DSRL. Daneben legte Art. 23 DSRL, der sich mit der Haftung im Sinne des Schadensersatzes befasste, ausdrücklich fest, dass hierfür nur der für die Verarbeitung Verantwortliche belangt werden konnte.[375] Art. 24 DSGVO, der die Umsetzung und die Sanktionen der DSRL regelte, bot weitergehenden Spielraum für die Mitgliedstaaten.[376] Dieser Spielraum galt auch für Art. 28 DSRL insoweit, wie das EU-Parlament im Gesetzgebungsverfahren zur DSRL annahm, dass die Eingriffsbefugnisse der Aufsichtsbehörden von der Rechtsform her Sanktionen seien.[377] Mangels expliziter Festlegung des Adressaten wurde vertreten, dass Stellen neben dem für die Verarbeitung Verantwortlichen Adressat der Untersuchungsbefugnisse sein können, so etwa der Lieferant oder Empfänger der (personenbezogenen) Daten.[378]

Ebenso wie in der Rechtssache Wirtschaftsakademie[379] wurde auch in Fashion ID dem EuGH die Frage vorgelegt, ob die DSRL ihren Adressaten abschließend festlege.[380]

---

[371] BT-Drs. 12/8329, S. 114 f.

[372] Vgl. a. zum BDSG 1990: BT-Drs. 11/4306, S. 53.

[373] BT-Drs. 12/8329, S. 42; für die verabschiedete Version scheinbar a.: Dammann/Simitis DSRL/*Dammann*, Art. 28, Rn. 10.

[374] Groeben, von der/Schwarze/*Gaitanides*, Art. 19 EUV, Rn. 47; Ehmann/Selmayr/*Selmayr/Ehmann*, Einleitung, Rn. 104.

[375] Siehe a.: ErwGr 55 S. 2 DSRL.

[376] Anders scheinbar Ehmann/Helfrich DSRL, Art. 24, Rn. 5, die zwar die offene Formulierung betonen, hier aber den für die Verarbeitung Verantwortlichen als (Haupt-)Anspruchsgegner sehen sowie ggf. die handelnde natürliche Person.

[377] BT-Drs. 12/8329, S. 42.

[378] Dammann/Simitis DSRL/*Dammann*, Art. 28, Rn. 9.

[379] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[380] EuGH, Urteil vom 05.06.2018 – C-210/16 (Wirtschaftsakademie) = ZD 2018, 357 Vorlagefrage 1.; EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977 Vorlagefrage 3.

Dabei hatte sich der Generalanwalt in den Schlussanträgen obiter dictum[381] dahingehend festgelegt, dass die Adressaten in der DSRL vollständig harmonisiert und somit abschließend geregelt seien.[382] In der dazugehörigen Vorlage hatte das OLG Düsseldorf noch die (zivilrechtliche) Inanspruchnahme eines Websitebetreibers, der ein Social Plugin eines Dritten in seine Webseite einbindet, aufgrund der damit verbundenen Datenerhebung als Störer[383] erwogen.[384] Der Generalanwalt erteilte diesem Vorstoß eine Absage, da er durch mitgliedstaatlichen Spielraum hinsichtlich der Adressaten divergierende Haftungsregime in den Mitgliedstaaten befürchtete. Der EuGH griff die Überlegungen des Generalanwalts im Urteil zu der Rechtssache Fashion ID nicht auf, sondern bemerkte, wiederum obiter dictum, dass eine zivilrechtliche Haftung für nicht verantwortete Verarbeitungsvorgänge nach dem Recht der Mitgliedstaaten nicht ausgeschlossen sei.[385] Wenn eine zivilrechtliche Haftung prinzipiell denkbar ist, ist allerdings nicht ersichtlich, warum eine Inanspruchnahme von Nichtstörern durch Aufsichtsbehörden kategorisch ausgeschlossen sein soll.[386] Daraus lässt sich, jedenfalls für die DSRL, folgern, dass eine eingeschränkte Form der Verantwortlichkeit für Verstöße im Zusammenhang mit einer Verarbeitung jenseits des für die Verarbeitung Verantwortlichen bestehen konnte. Mangels einer Begründung des EuGH ist allerdings nicht klar, aus welchem normativen Kontext dieser den Spielraum für eine zivilrechtliche Haftung begründet. Folglich lassen sich auch keine definitiven Schlüsse auf die Übertragbarkeit dieser Feststellungen des EuGH von der DSRL auf die DSGVO ziehen. Da die DSRL zum Zeitpunkt des Urteils in der Rechtssache Fashion ID Mitte 2019 allerdings nur noch Bedeutung für Altfälle hatte, liegt es nahe, dass der EuGH eine Klarstellung für die DSGVO ergänzt hätte, wenn diese notwendig gewesen wäre.

Folglich war zwar grundsätzlich der für die Verarbeitung Verantwortliche Adressat der DSRL. Die DSRL war aber nicht zwingend nur auf diesen festgelegt. Ob andere Adressaten denkbar waren, war im Hinblick auf die einzelne Norm zu ermitteln.[387] Im Hinblick auf die sehr weite Formulierung des Art. 24 DSRL schien es denkbar hiermit

[381] Ausgehend davon, dass der Websitebetreiber gemeinsam Verantwortlicher sei, beantwortet der Generalanwalt die Vorlagefrage bezüglich der abschließenden Regelung nur (quasi-)obiter dictum.

[382] EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 110. Dabei scheint der Generalanwalt Haftung und Verantwortlichkeit gleichzusetzen.

[383] Gemeint ist die zivilrechtliche Störerhaftung: OLG Düsseldorf, Beschluss (Vorlage EuGH) vom 19.01.2017 – I-20 U 40/16 = GRUR 2017, 416, Rn. 15 f.

[384] Vorlagefrage 3. und OLG Düsseldorf, Beschluss (Vorlage EuGH) vom 19.01.2017 – I-20 U 40/16 = GRUR 2017, 416, Rn. 15 f.

[385] EuGH, Urteil vom 29.07.2019 – C-40/17 (Fashion ID) = GRUR 2019, 977, Rn. 74. Mit Nachweisen für eine solche Haftung: *Hense*, DSB[44] (2020), 236, 237.

[386] Vgl. a. die Erwägungen zum Zweckveranlasser in Kapitel 5 J. Störerhaftung und Zweckveranlasser.

[387] Vgl. EuGH, Schlussanträge vom 19.12.2018 – C-40/17 (Fashion ID), Rn. 41.

auch weitere Adressaten für einzelne Normen festzulegen.[388] Dies galt gerade deswegen, weil die Durchführungspflicht aus Art. 24 DSRL auch den Vollzug erfasste.[389]

VII. Fazit

Betrachtet man die Systematik der DSGVO, das Urteil des EuGH in der Rechtssache Fashion ID sowie die Vorgängernorm von Art. 58 Abs. 2 lit. f DSGVO scheint die Annahme des Verantwortlichen als einzigem Normadressat, soweit ein solcher nicht ausdrücklich genannt wird, problematisch. Gleichwohl verwundert es, dass ein Normadressat nicht unmittelbar ersichtlich ist. Nimmt man an, dass ein Rückgriff auf die Adressaten des allgemeinen Polizei- und Ordnungsrechts und damit auch Zweckveranlasser und Nichtstörer möglich ist, stellt sich allerdings die Frage, inwiefern damit viel für das Verantwortlichkeitskonzept der DSGVO gewonnen ist.

Dabei steht zur Debatte, inwiefern ein solcher Rückgriff bei einer sehr weiten Auslegung der gemeinsamen Verantwortlichkeit überhaupt notwendig ist. Sinnvollerweise sollte ein solcher Rückgriff an die Stelle von Grenzfällen der gemeinsamen Verantwortlichkeit treten. Allerdings ist fraglich, inwiefern ein nationaler Sonderweg mit der Rechtsprechung des EuGH zu vereinbaren wäre. Im Zweifel bestünde für das Unionsrecht Anwendungsvorrang gegenüber dem Recht des Mitgliedstaats. Unabhängig vom Verhältnis eines solchen Rückgriffs zur gemeinsamen Verantwortlichkeit würde dies aber auch zu einer Rechtszersplitterung zwischen den Mitgliedstaaten führen. Eine eigene Regelung einzelner Mitgliedstaaten hinsichtlich einer Haftung für vor- und nachgelagerte Verarbeitungsvorgänge, soweit keine Verantwortlichkeit besteht, erscheint aber nach der Rechtsprechung des EuGH unproblematisch.

Der Zugriff der Aufsichtsbehörde auf Akteure, die nicht Verantwortliche oder Auftragsverarbeiter für die fragliche Verarbeitung sind, mag zudem Extremfälle von Datenschutzverstößen verhindern können, allerdings handelt es sich aufgrund der Natur der Befugnis nur um eine reaktive Maßnahme. Als solche setzt sie eine entsprechende Kenntnis oder vorhergehende Prüfung der Verarbeitung durch die Aufsichtsbehörde voraus. Ein weites Verständnis der Adressaten in Art. 58 Abs. 2 lit. f DSGVO könnte aber, abseits der Möglichkeit einer zivilrechtlichen Haftung nach nationalem Recht als Abschreckungseffekt, datenschutzrechtliche Verstöße und somit auch Schäden bereits vermeiden, anstatt sie nur zu sanktionieren.

---

[388] Vgl. Dammann/Simitis DSRL/*Dammann*, Art. 24, Rn. 1, 4, insb. wegen der Änderung von Art. 24 vom geänderten Vorschlag (BT-Drs. 12/8329, S. 106) zur endgültigen Fassung.

[389] Dammann/Simitis DSRL/*Dammann*, Art. 24, Rn. 2; Grabitz/Hilf[40]/*Brühann*, A 30 Art. 24 DSRL, Rn. 7.

Eine Feinsteuerung des Verantwortlichkeitskonzeptes und seiner Rollen wird mit einem weiten Verständnis des Adressaten in Art. 58 Abs. 2 lit. f DSGVO allerdings gerade nicht erreicht. Im Gegenteil, durch die Erstreckung dieser Abhilfebefugnis auf den Nichtstörer würden, jedenfalls potenziell, auch gänzlich Unbeteiligte erfasst. Dabei ist gleichermaßen zu bedenken, dass alle Akteure außer dem Verantwortlichen oder Auftragsverarbeiter ohnehin nach datenschutzrechtlichem Verständnis Unbeteiligte sind. Auf rein pragmatischer Ebene wäre eine weite Auslegung von Art. 58 Abs. 2 lit. f DSGVO aber im Gegensatz zu einer legislativen Ausdifferenzierung des Verantwortlichkeitskonzeptes eine kurzfristig realisierbare Maßnahme. Allein im Hinblick auf Verständlichkeit und Systematik der Norm erscheint es trotzdem sinnvoll, Art. 58 DSGVO langfristig um einen allgemeinen Adressaten zu ergänzen und Abweichungen in den einzelnen Befugnissen aufzugreifen.

L. Ausblick

Wie und vor allem wann sich das Verantwortlichkeitskonzept der DSGVO weiterentwickeln wird, scheint momentan völlig unklar. Die erste Evaluation der DSGVO aus dem Mai 2020, wie sie Art. 97 Abs. 1 DSGVO vorsieht, hat hinsichtlich der Verantwortlichkeit keine Feststellungen gemacht. Seite 19 der Evaluation sieht allein vor, dass der Ausschuss, also der EDPB, und die Datenschutzbehörden ersucht werden „die Harmonisierung bei der Anwendung und Durchsetzung der DSGVO unter Nutzung aller ihr zur Verfügung stehenden Mittel zu unterstützen, unter anderem durch eine weitere Klarstellung der Schlüsselkonzepte der DSGVO [...]“.[390] Unter diese Schlüsselkonzepte dürfte auch die Verantwortlichkeit fallen. So wird im Commission Staff Working Document festgestellt, dass zwischen den deutschen Aufsichtsbehörden das Verständnis des Verantwortlichen und des Auftragsverarbeiters unterschiedlich kommuniziert wird.[391] Tatsächliche Feststellungen zu einem Reformbedarf finden sich in der Evaluation allerdings nicht. Die nächste Evaluation wird erst im Mai 2024 stattfinden.[392] Unabhängig von einer solchen Evaluation scheint ein Tätigwerden der Kommission extrem unwahrscheinlich. Dies gilt insbesondere im Hinblick auf die noch ausstehende ePrivacy-VO sowie den komplizierten Gesetzgebungsprozess der DSGVO selbst.

[390] *Europäische Kommission*, Mitteilung der Kommission an das Europäische Parlament und den Rat, 24.06.2020, 19.

[391] *Europäische Kommission*, Commission Staff Working Document, 24.06.2020, 10.

[392] Zur Drucklegung dieser Arbeit waren noch keine Ergebnisse bekannt.

Daneben wird in der Evaluation festgestellt, dass die Stakeholder weiterführende Leitlinien hinsichtlich des Verständnisses des Verantwortlichen, der gemeinsam Verantwortlichen und des Auftragsverarbeiters fordern. Die neuen Leitlinien zum Verantwortlichen und Auftragsverarbeiter hat der EDPB im Juli 2021 veröffentlicht.[393] Dabei orientiert er sich im Wesentlichen am WP 169 seines Vorgängergremiums, der Art. 29-Datenschutzgruppe, und der Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit. Tiefergreifende Analysen zu den einzelnen Definitionselementen des Verantwortlichen oder der gemeinsam Verantwortlichen finden sich dort nicht. Nach dieser Veröffentlichung der finalen Version der Leitlinien dürfte vom EDPB abseits einer spezifischen Überarbeitungsabsicht der DSGVO durch die Kommission kein neues Konzept zu erwarten sein.

Ein Tätigwerden des nationalen Gesetzgebers im Rahmen der Spezifizierungs- bzw. Öffnungsklauseln der DSGVO scheint auch nicht absehbar. So tut sich der deutsche Gesetzgeber bereits bei den wichtigen Spezifizierungsklauseln der Art. 85 DSGVO bezüglich der Meinungs- und Pressefreiheit sowie bei Art. 88 DSGVO hinsichtlich des Beschäftigtendatenschutzes schwer, über den status quo der DSRL hinaus weiter tätig zu werden. Hinsichtlich des durchaus eingeschränkten Spielraums im Hinblick auf die Verantwortlichkeit oder die aufsichtsbehördlichen Befugnisse scheint dort ein Tätigwerden kaum zu erwarten zu sein.

Denkbar wäre, dass der EuGH seine Rechtsprechung zur gemeinsamen Verantwortlichkeit weiter konkretisiert. Andererseits scheint dies im Rahmen der fünf bereits ergangenen Entscheidung hierzu, also Wirtschaftsakademie, Jehovan todistajat, Fashion ID, NZÖG und IAB Europe[394] eher unwahrscheinlich. Gerade die Entscheidung IAB Europe zog weitestgehend nur ein Resümee der vorherigen Entscheidungen.[395] So ist der EuGH bislang auch nicht auf die entscheidenden Definitionselemente der Zwecke und Mittel bei der gemeinsamen Verantwortlichkeit detailliert eingegangen.[396] Das Merkmal der Entscheidung streifte der EuGH in der Rechtssache NZÖG nur.[397] Sofern der EuGH weiter Schutzdefizite bei der DSGVO erkennt, dürfte er eher die gemeinsame Verantwortlichkeit weiter ausweiten, als eine neue Form der Verantwortlichkeit oder Haftung einzuführen. Realistisch scheint neue Rechtsprechung des EuGH indes vor allem zu den Voraussetzungen der Haushaltsausnahme, gerade im

[393] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021.

[394] Dazu: Kapitel 4 B. Rechtsprechung des EuGH.

[395] EuGH, Urteil vom 07.03.2024 – C-604/22 (IAB Europe) = ZD 2024, 328, Rn. 55 ff.

[396] Kritisch auch: *Schneider*, Gemeinsame Verantwortlichkeit, 2021, 74 f.

[397] EuGH, Urteil vom 05.12.2023 – C-683/21 (NZÖG) = ZD 2024, 209, Rn. 43.

Hinblick auf ErwGr 18 S. 2 der DSGVO. Eine Entscheidung des EuGH würde aber wiederum voraussetzen, dass die nationalen Aufsichtsbehörden gewillt sind, entsprechende Verfahren anzustrengen und die Verantwortlichen solche Verfahren mittragen. Denkbar erscheint aber auch ein Vorgehen von Verbraucherschutzverbänden gegenüber Verantwortlichen gem. Art. 80 Abs. 2 DSGVO.

Insgesamt stehen die Chancen für eine umfassende Überarbeitung des Konzeptes der Verantwortlichkeit in der DSGVO eher schlecht. Daher soll diese Arbeit vor allem eine Analyse des status quo erbringen und denkbare, wenn auch nicht immer unproblematische, Optionen abseits eines Tätigwerdens des Unionsgesetzgebers aufzeigen. Auch wenn die Chancen hierfür eher schlecht stehen, stellt die dringendste Erkenntnis aus dieser Arbeit die Notwendigkeit einer weiteren Ausdifferenzierung der Verantwortlichkeitsrollen da. Abseits weiterer Zwischenstufen zwischen dem Verantwortlichen und einem datenschutzrechtlichen Nullum sollten auch Verantwortlichkeitsrollen für spezifische Verarbeitungskontexte erwogen werden. Diese könnten im Kontext anderer Regelungswerke (etwa dem European Health Data Space) Eingang finden und die bestehenden Rollen der DSGVO modifizieren. Dies würde schließlich auch der Bezeichnung der DSGVO als Datenschutz**grund**verordnung gerecht. Sollte der Unionsgesetzgeber tatsächlich tätig werden, empfiehlt es sich solche und andere Ansätze zeitlich zu befristen und entsprechend zu evaluieren.[398] Dies gilt auch dahingehend, eine erneute Pfadabhängigkeit, wie sie vor allem die historische Dimension des Verantwortlichen zeigt, zu verhindern. Abschließen soll diese Arbeit daher mit einem eher rechtstechnischen Zitat aus den OECD-Guidelines aus dem Jahr 1980 sowie einem pragmatischen Zitat von Simitis als Appell an die verschiedenen Stakeholder:

> *„In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities.“*[399]

> *„Modernisierungen sind, anders und schärfer ausgedrückt, nicht mehr als Zwischenstationen eines unverändert offenen Regelungsprozesses.“*[400]

[398] *Lennartz*, RdV 1990, 25, 28 f.

[399] *Organisation for Economic Co-operation and Development*, Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data, 23.09.1980, Rn. 40.

[400] Simitis/*Simitis*, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 106.

Kapitel 6

Zusammenfassung in Thesen

Im Rahmen der Analyse der vorangegangenen Abschnitte wurden verschiedene Aspekte der Verantwortlichkeit analysiert. Hier werden die wesentlichen Thesen im Einzelnen und der Gliederung der Arbeit folgend festgehalten:

A. Zu Kapitel 1: Grundlagen zum Konzept des Verantwortlichen

1. Die Definition des Dritten dient indirekt, durch die Bestimmung der Verantwortlichkeitssphäre des Verantwortlichen, der Bestimmung anderer Verantwortlicher.
2. Die Definition des Verantwortlichen nach DSRL und DSGVO ist inhaltlich identisch. Die Rechtsprechung und Literatur zum für die Verarbeitung Verantwortlichen gem. Art. 2 lit. d DSRL lässt sich grundsätzlich auf die DSGVO übertragen.
3. Die Verpflichtung des Verantwortlichen auf die Grundsätze der Verarbeitung in Art. 5 Abs. 2 DSGVO im Rahmen der Rechenschaftspflicht kommt nicht einer Festlegung des Verantwortlichen als allgemeinem Adressaten der DSGVO gleich.
4. Der Verantwortliche wird entweder direkt, durch explizite Erwähnung, oder indirekt, durch Verweis auf eine andere Norm, in der er explizit erwähnt wird, als Adressat verpflichtet.
5. Der Verantwortliche hat keine entscheidende Bedeutung für andere zentrale Konzepte der DSGVO wie den räumlichen Anwendungsbereich. Daher leitet sich daraus auch nicht eine Stellung des Verantwortlichen als vermeintlich allgemeinem Adressaten der DSGVO ab.
6. Das Konzept der Verantwortlichkeit im Datenschutz hat seit seiner Genese in den 70er Jahren nur geringfügige Änderungen erfahren. Man kann es daher als strukturkonservativ bezeichnen.
7. Die wesentlichsten Änderungen des Konzeptes der Verantwortlichkeit waren die Abkehr vom Bezugsobjekt der Datei, das Abstellen auf die Entscheidung über die Zwecke und Mittel der Verarbeitung als Voraussetzung der Verantwortlichkeit sowie die Einführung der gemeinsam Verantwortlichen durch die DSRL im Jahr 1995.

8. Die Definition der verantwortlichen Stelle in § 3 Abs. 7 BDSG 2001 musste mangels Erwähnung der Entscheidung über die Zwecke und Mittel der Verarbeitung sowie der gemeinsam Verantwortlichen unionsrechtskonform ausgelegt werden.

9. Aufgrund des alleinigen Bezugs auf die Verarbeitung war die Definition der verantwortlichen Stelle in § 3 Abs. 7 BDSG wenigstens im Wortlaut weiterhin einer technischen Sichtweise hinsichtlich der Bestimmung des Verantwortlichen verhaftet.

10. Die Verarbeitungsrealität hat sich seit der Konzeption des Datenschutzrechts in den 70er Jahren maßgeblich verändert und bedingt nun dringend eine Anpassung des Konzeptes der Verantwortlichkeit.

B. Zu Kapitel 2: Definitionselemente des Verantwortlichen und Abgrenzung

11. Die Bestimmung eines singulär Verantwortlichen ist regelmäßig unproblematisch.

12. Der Begriff des Verantwortlichen muss unionsrechtsautonom ausgelegt werden.

13. Bezugsobjekt der Verantwortlichkeit ist regelmäßig der individuelle Verarbeitungsvorgang. Mehrere Verarbeitungsvorgänge können allerdings auch unter einem übergreifenden Zweck als Vorgangsreihe zusammengefasst werden.

14. Der Begriff der Stelle konturiert den Verantwortlichen. Er bestimmt unter anderem die zur Verarbeitung privilegierten Personen gem. Art. 29 DSGVO und ist maßgeblich für die Haftung nach Art. 82 DSGVO sowie für die Verhängung von Geldbußen gem. Art. 83 DSGVO. Die Stelle ist regelmäßig eine Organisationseinheit und nicht eine natürliche Person.

15. Die Zurechnung des Verhaltens der dem Verantwortlichen unterstellten Personen erfolgt im Rahmen der Weisungsgebundenheit gem. Art. 29 DSGVO. Dies gilt allerdings nicht für den Fall eines Mitarbeiterexzesses.

16. Die Konturierung der Stelle in Konzernstrukturen wird nicht durch das Kartell- oder Gesellschaftsrecht vorgegeben, sondern bestimmt sich vielmehr nach der Entscheidungsautonomie der beteiligten Gesellschaften.

17. Eine Niederlassung oder ein Vertreter im Unionsgebiet stellen nicht notwendigerweise eine Stelle dar.

18. Das Definitionselement der Stelle hängt eng mit dem Definitionselement der Entscheidung zusammen.

19. Der Zweck in der Definition des Verantwortlichen bezieht sich systematisch auf den Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b DSGVO.

20. Die Mittel teilen sich in wesentliche Elemente und unwesentliche Elemente auf. Wesentliche Elemente betreffen die personenbezogenen Daten als solche, unwesentliche Elemente betreffen technische und organisatorische Fragen. Die Differenzierung zwischen wesentlichen und unwesentlichen Elementen ergibt sich auch aus Art. 28 Abs. 3 DSGVO.

21. Im Rahmen der Entscheidung über eine zu verwendende Soft- oder Hardware kann indirekt auch eine Entscheidung über wesentliche Elemente der Mittel erfolgen.

22. Die Kenntnis der Zwecke für die Entscheidung über diese ergibt sich aus der Notwendigkeit der Zweckfestlegung. Eine Kenntnis der Mittel für die Entscheidung ist bei einem singulär Verantwortlichen nicht notwendig.

23. Bei gemeinsam Verantwortlichen ist für die Entscheidung über die Mittel wenigstens ein Kennenmüssen im Sinne einer grob fahrlässigen Unkenntnis erforderlich.

24. Bei Kindern und Personen unter rechtlicher Betreuung ist eine Entscheidungsfähigkeit Voraussetzung für eine Entscheidung über die Zwecke und Mittel. Die Entscheidungsfähigkeit setzt ein zumindest abstrakt mögliches Verständnis der Kausalzusammenhänge zwischen dem eigenen Handeln und der daraus folgenden Verarbeitung voraus. Dies schließt ein Verständnis des Zweckes und ein grobes Verständnis der Mittel ein.

25. Die Entscheidung setzt keine besondere Form voraus. Für die Verarbeitung durch einen Auftragsverarbeiter ist der Vertrag nach Art. 28 Abs. 3 DSGVO nicht konstitutiv, für die Verarbeitung durch gemeinsam Verantwortliche die Vereinbarung nach Art. 26 Abs. 1 S. 2 DSGVO nicht konstitutiv.

26. Der Verantwortliche muss die Verarbeitung nicht selbst technisch beeinflussen können, er muss sie allerdings indirekt kontrollieren können. Entbehrlich ist bei gemeinsam Verantwortlichen ein individueller Zugriff auf die verarbeiteten Daten.

27. Der alleinige Eindruck bzw. die Erwartungen einer betroffenen Person über die Verantwortlichkeit eines Akteurs führt nicht bereits zu einer tatsächlichen Verantwortlichkeit dieses Akteurs.

28. Maßgeblich für die Entscheidung über die Zwecke und Mittel einer Verarbeitung sind die tatsächlichen Umstände. Eine explizite Zuständigkeit qua Gesetz oder Vertrag sowie eine implizite Zuständigkeit qua Aufgaben können nur Indiz für eine

Entscheidung sein. Dies gilt aber nicht für die Benennung des Verantwortlichen nach Art. 4 Nr. 7 2. Hs. DSGVO.

29. Die Benennung eines Verantwortlichen bzw. die Kriterien für seine Benennung können im Rahmen der Verarbeitungsrechtfertigungstatbestände gem. Art. 6 Abs. 1 lit. c und e DSGVO vorgesehen werden. Dabei müssen allerdings die notwendigen Definitionselemente wie die Zwecke und die wesentlichen Elemente der Mittel der Verarbeitung festgelegt werden.

30. Fallen gesetzlich benannter Verantwortlicher und tatsächlicher Verantwortlicher auseinander, ist im Zweifel von der gesetzlichen Verantwortlichkeit auszugehen.

31. Die Abgrenzung von Verantwortlichen und Auftragsverarbeitern erfolgt anhand der Weisungsgebundenheit und des Entscheidungsspielraums des Auftragsverarbeiters.

32. Das Eigeninteresse eines vermeintlichen Auftragsverarbeiters an einer Verarbeitung ist kein sicheres Kriterium für eine Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter. Denn das Eigeninteresse kann auch in der Entlohnung oder späteren Verarbeitung der erlangten Daten liegen.

C. Zu Kapitel 3: Folgen der Verantwortlichkeit

33. Für eine gesamtschuldnerische Haftung nach Art. 82 Abs. 4 DSGVO muss nicht zwangsläufig eine gemeinsame Verantwortlichkeit bestehen.

34. Das Verhältnis zwischen DSGVO und DSA ist weiter klärungsbedürftig. Ob und inwieweit die Haftungsprivilegierungen innerhalb des DSA auf die DSGVO anwendbar sind, ist unklar.

35. Der für Art. 83 DSGVO anzuwendende funktionale Unternehmensbegriff wird nur für die Bemessung der Geldbuße relevant. Er hat keine weitere Rückwirkung auf die Verantwortlichkeit.

36. Aufgrund des unionsrechtsautonomen Verständnisses der Verantwortlichkeit sind die weiteren materiellen Erfordernisse des OWiG im Kontext einer Geldbuße nach Art. 83 DSGVO unionsrechtswidrig.

D. Zu Kapitel 4: Gemeinsam mit anderen (Verantwortlichen)

37. Die Weiterleitung zwischen mehreren speicherberechtigten Stellen nach § 6 Abs. 2 BDSG a.F. stellte keine Umsetzung der gemeinsamen Verantwortlichkeit der DSRL dar.

38. Art. 4 Nr. 7 DSGVO und Art. 26 Abs. 1 S. 1 DSGVO definieren die gemeinsam Verantwortlichen inhaltlich identisch.

39. Der Definitionsteil mit „anderen" bezieht sich auf Dritte gem. Art. 4 Nr. 10 DSGVO.

40. Bezugsobjekt des Definitionselements „gemeinsam" ist die Entscheidung, nicht die Zwecke oder Mittel der Verarbeitung.

41. Gemeinsam Verantwortliche stellen kein selbstständiges Rechtssubjekt neben oder statt ihrer individuellen Verantwortlichkeit dar.

42. Divergieren die Zwecke zwischen gemeinsam Verantwortlichen, so können auch unterschiedliche Vorgangsreihen für die individuellen gemeinsam Verantwortlichen vorliegen. Bei gemeinsamen Zwecken kann eine Vorgangsreihe auch über verschiedene Vorgänge der individuell gemeinsam Verantwortlichen hinweg bestehen.

43. Die absolute Grenze der Abstraktion von Verarbeitungsvorgängen zu einer Vorgangsreihe ist der Zweckbindungsgrundsatz.

44. Die Vorgangsreihe bündelt unterschiedliche Verarbeitungsvorgänge, nicht aber unterschiedliche Zwecke zwischen verschiedenen Verantwortlichen.

45. Das gemeinsame „(wirtschaftliche) Interesse" im Urteil des EuGH zu Fashion ID ist als Zweckkomplementarität zwischen den Verantwortlichen zu verstehen.

46. Die Zweckkomplementarität indiziert eine Billigungsfähigkeit fremder Zwecke unter gemeinsam Verantwortlichen. Bei einer Durchführung der Verarbeitung liegt dann eine Billigung vor.

47. Gemeinsame Zwecke sind isoliert betrachtet nicht erforderlich für eine gemeinsame Verantwortlichkeit.

48. Gemeinsame Mittel sind isoliert betrachtet nicht erforderlich für eine gemeinsame Verantwortlichkeit.

49. Die Billigung fremder Zwecke oder Mittel ist erforderlich für eine gemeinsame Entscheidung. Sie muss im Rahmen einer Entscheidungsautonomie erfolgen. Eine explizite Billigung ist bei bestehender Komplementarität der Zwecke oder Mittel nicht erforderlich. Eine Missbilligung fremder Zwecke oder Mittel hingegen muss nach

außen ersichtlich sein. Die Billigung bezieht sich auf Verarbeitungsvorgänge oder Vorgangsreihen. Diese müssen zwischen den gemeinsam Verantwortlichen identisch sein.

50. Ein Zu-Eigen-Machen fremder Zwecke oder Mittel stellt einen eigenen Entscheidungsbeitrag dar und nicht nur eine Billigung. Das Zu-Eigen-Machen geht über eine bloße Hinnahme fremder Zwecke oder Mittel hinaus. Bei den Mitteln ist es regelmäßig in der Durchführung der Verarbeitung zu erkennen.

51. Eine reine Billigung fremder Zwecke und Mittel führt nicht zu einer gemeinsamen Verantwortlichkeit.

52. Gemeinsame Zwecke oder Mittel fungieren als Identitätsgarant einer gemeinsamen Verantwortlichkeit.

53. Im Rahmen der gemeinsamen Entscheidung muss ein Entscheidungsbeitrag zu den Zwecken oder Mitteln der Verarbeitung bestehen. Dieser kann auch in einem Zu-Eigen-Machen liegen. Auch die Ermöglichung einer Verarbeitung ist ein solcher Entscheidungsbeitrag. Ein Entscheidungsbeitrag liegt in jedem Fall dann vor, wenn die Verarbeitung ohne diesen anders ausgefallen wäre.

54. Die gemeinsame Entscheidung ist nicht prozessbezogen, sondern ergebnisbezogen zu verstehen. Daher reicht ein arbeitsteiliges Vorgehen der gemeinsam Verantwortlichen. Eine Abstimmung im Sinne eines einheitlichen, konsensualen Prozesses ist nicht notwendig.

55. Die Erheblichkeitsschwelle des Entscheidungsbeitrags eines gemeinsam Verantwortlichen ergibt sich aus den Festlegungserfordernissen für die Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO. Sofern ein Entscheidungsbeitrag vorliegt, der nicht im Entscheidungsspielraum eines Auftragsverarbeiters liegt, ist dies für die gemeinsame Entscheidung ausreichend. Dies gilt allerdings nur so weit, wie ein Auftragsverarbeiter an der Verarbeitung beteiligt ist. Ohne einen Auftragsverarbeiter reicht jeder Entscheidungsbeitrag hinsichtlich der Zwecke und Mittel der Verarbeitung.

56. Ein ja/nein-Entscheidungsspielraum ist für einen Entscheidungsbeitrag ausreichend.

57. Ein Entscheidungsbeitrag kann auch in einem Unterlassen bestehen, sofern dies erheblich für die Durchführung der Verarbeitung ist. Denkbar ist hier die Duldung einer Verarbeitung durch das Gewähren der Nutzung von Daten oder Infrastruktur.

58. Eine gemeinsame Verantwortlichkeit ist keine zwingende Folge eines Auftragsverarbeiterexzesses. Eine Billigung der fremden Zwecke oder Mittel des ehemaligen Auftragsverarbeiters ist erforderlich.

59. Die Figur der Funktionsübertragung ist mit der Normierung des Auftragsverarbeiterexzesses in Art. 28 Abs. 10 DSGVO obsolet geworden.

60. Die Befolgung gesetzlicher Übermittlungspflichten auf Basis von EU-/EWR-Recht führt nicht zu einem Auftragsverarbeiterexzess. Die Befolgung solcher Pflichten aufgrund von Nicht-EU- oder Nicht-EWR-Recht hingegen schon.

61. Die Voraussetzungen eines Mitarbeiterexzesses gem. Art. 29 DSGVO bestehen analog zum Auftragsverarbeiterexzess gem. Art. 28 Abs. 10 DSGVO.

62. Die gemeinsam Verantwortlichen sind untereinander hinsichtlich des Erfordernisses einer Verarbeitungsrechtfertigung nicht privilegiert.

63. Die Reichweite der individuellen Verantwortung eines gemeinsam Verantwortlichen bestimmt sich anhand der konkret mitverantworteten Verarbeitungsvorgänge. Durch diesen vorgangsorientierten Ansatz leidet allerdings die Transparenz gegenüber der betroffenen Person. Auch praktisch ergeben sich Probleme hinsichtlich der Informationspflichten und der Einwilligung.

64. Das Verhältnis der individuellen Verantwortung eines gemeinsam Verantwortlichen wird im Rahmen der Bemessung von Geldbußen gem. Art. 83 DSGVO sowie beim Regress der gemeinsam Verantwortlichen untereinander gem. Art. 82 Abs. 5 DSGVO erheblich.

65. Art. 26 Abs. 3 DSGVO führt nicht zu einer gesamtschuldnerischen Verantwortlichkeit der gemeinsam Verantwortlichen, sondern zu einer Einwirkungs- und Weiterleitungspflicht.

66. Gemeinsam Verantwortliche müssen nicht autonom sämtlichen Pflichten der DSGVO nachkommen können.

67. Eine Delegation von bestimmten Pflichten der DSGVO ist bei gemeinsam Verantwortlichen möglich. Die Möglichkeit der Delegation hängt davon ab, ob die Pflicht die Verarbeitung betrifft oder die Verantwortlichen individuell. Fehlt eine Vereinbarung über die Verteilung der Pflichten, kann die Pflicht von jedem gemeinsam Verantwortlichen eingefordert werden.

68. Die Störerauswahl bei gemeinsam Verantwortlichen orientiert sich am Primat der Effektivität der Gefahrenabwehr.

69. Die Voraussetzungen der gemeinsamen Verantwortlichkeit sind weder aus der DSGVO noch aus der Rechtsprechung des EuGH bislang eindeutig abzuleiten.

70. Die gemeinsame Verantwortlichkeit ist zu stark auf die betroffene Person ausgerichtet. Die Möglichkeit einer Abstufung der Verantwortlichkeit ist dringend erforderlich. Dazu müssen die Verantwortlichkeitsrollen ausdifferenziert werden.

71. Die weite Auslegung der gemeinsamen Verantwortlichkeit durch den EuGH wird langfristig nicht durchzuhalten sein.

E. Zu Kapitel 5: Ansätze zur Überarbeitung des Konzeptes der Verantwortlichkeit

72. Die durchgehende Annahme singulär Verantwortlicher ist aufgrund der technologischen und organisatorischen Entwicklung nicht mehr haltbar.

73. Eine Typologie verschiedener Verantwortlichkeitsrollen könnte langfristig zu einer gesetzgeberischen Ausdifferenzierung führen.

74. Eine Auswahlverantwortlichkeit könnte die reine Ermöglichung fremder Verarbeitungen angemessen einhegen.

75. Eine „datenschutzrechtliche Beihilfe" könnte Szenarien abdecken, in denen ein Akteur nur über unwesentliche Elemente der Mittel entscheidet, allerdings nicht weisungsgebunden und somit kein Auftragsverarbeiter ist.

76. Eine Herstellerverantwortlichkeit besteht nach geltendem Recht nicht. Je nach konkreter Ausgestaltung könnte sie allerdings den Anwendungsbereich der gemeinsamen Verantwortlichkeit einschränken. Denkbar wäre dabei jedenfalls die Verpflichtung auf bestimmte Grundsätze der Verarbeitung gem. Art. 5 Abs. 1 DSGVO.

77. Eine isolierte Intermediärsverantwortlichkeit ist bislang nicht erforderlich. Notwendig wäre es hingegen, die Verantwortlichkeit von Intermediären für die Inhalte ihrer Nutzer sowie das Verhältnis von DSGVO zum DSA zu klären.

78. Ein breiteres Verständnis der Haushaltsausnahme in Art. 2 Abs. 2 lit. c DSGVO könnte dazu beitragen die Anwendungsfälle der gemeinsamen Verantwortlichkeit zu reduzieren. Bislang ist allerdings unklar, ob der EuGH seine Rechtsprechung aus den Rechtssachen Lindqvist und Rynes revidieren wird. Daneben ist auch unsicher, wie sich die Anwendbarkeit der Haushaltsausnahme zur gemeinsamen Verantwortlichkeit und Auftragsverarbeitung verhält. Es liegt nahe davon auszugehen, dass nur die Verantwortlichkeit der privilegierten Person entfällt, die Verantwortlichkeit bzw. Auftragsverarbeitung der anderen Akteure aber ansonsten bestehen bleibt.

79. Nach dem Urteil des EuGH in der Rechtssache Fashion ID ist eine weitergehende zivilrechtliche Haftung eines Akteurs für der Verarbeitung vor- oder nachgelagerte Verarbeitungen, für die er nicht Verantwortlicher ist, nach mitgliedstaatlichem Recht möglich. Allerdings sind dabei noch viele Folgefragen offen. Schlüssig erscheint neben einer potenziellen Anwendung der Störerhaftung auch die der Figur des Zweckveranlassers. Deren jeweilige Anwendung könnte bis zu einer Überarbeitung des Konzeptes der Verantwortlichkeit eine sinnvolle Zwischenlösung darstellen.

80. Ein Rückgriff auf die Störer des allgemeinen Polizei- und Ordnungsrechts bei Maßnahmen der Aufsichtsbehörden, die keinen Adressaten benennen, wäre grundsätzlich denkbar. Er wäre allerdings keineswegs unproblematisch. Sinnvoll erscheint ein Rückgriff vor allem hinsichtlich der Inanspruchnahme des Zweckveranlassers und des Nichtpflichtigen.

81. Die DSGVO stellt jedenfalls hinsichtlich ihrer aufsichtsbehördlichen Dimension Gefahrenabwehrrecht im Sinne der deutschen verwaltungsrechtlichen Systematik dar.

82. Mangels expliziter oder impliziter Benennung eines Adressaten regelt Art. 58 Abs. 2 lit. f DSGVO diesen nicht abschließend.

83. Von den Unionsgesetzgeber dürfte in absehbarer Zeit keine grundlegende Überarbeitung des Konzeptes der Verantwortlichkeit zu erwarten sein. Der nationale Gesetzgeber hat kaum Spielraum und war historisch gesehen bislang ohnehin zaghaft hinsichtlich der Öffnungsklauseln. Auch der EDPB wird nach den Leitlinien zum Verantwortlichen und Auftragsverarbeiter keine Grundsatzdebatte anstoßen. Denkbar dürfte vor allem eine weitere Ausdifferenzierung der gemeinsamen Verantwortlichkeit sowie der Haushaltsausnahme durch den EuGH sein.

Literaturverzeichnis

Abel, Ralf-Bernd, 2.7 Geschichte des Datenschutzrechts, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 194–217.

Albers, Marion, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, 2. Aufl. München 2012, 107–234.

–, § 62 Datenschutzrecht, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, 4. Aufl. Heidelberg 2020, 1148–1189.

–, § 22 Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle, Andreas/Eifert, Martin/Möllers, Christoph (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, 3. Aufl. München 2022, 1587–1660.

Albrecht, Jan Philipp, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343en.pdf, Stand: 16.01.2013, zuletzt abgerufen: 17.07.2024.

–, Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343de.pdf, Stand: 16.01.2013, zuletzt abgerufen: 17.07.2024.

Albrecht, Jan Philipp/Jotzo, Florian, Das neue Datenschutzrecht der EU: Grundlagen, Gesetzgebungsverfahren, Synopse, Baden-Baden 2017.

Alich, Stefan/Nolte, Georg, Zur datenschutzrechtlichen Verantwortlichkeit (außereuropäischer) Hostprovider für Drittinhalte, CR 2011, 741–745.

Alsenoy, Brendan van, Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EG, CLSR[28] (2012), 25–43.

–, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection, JIPITEC[7] (2016), 271–288.

–, Regulating Data Protection: The Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing, Leuven 2016.

Ambrock, Jens, Mitarbeiterexzess im Datenschutzrecht: Verantwortlichkeit und Haftung für Verstöße gegen die DS-GVO durch Beschäftigte, ZD 2020, 492–497.

Artikel-29-Datenschutzgruppe, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen 2008.

–, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke 2009.

–, Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten 2009.

–, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" 2010.

–, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679 2017.

Augsberg, Ino, Verantwortung als Reflexion: Die Konstruktion multilateraler Verantwortung im Informationsverbund, RW 2019, 109–122.

Ausloos, Jef, The Right To Erasure: Safeguard For Informational Self-Determination In A Digital Society?, Leuven 2018.

Bäcker, Matthias, D. Polizeiaufgaben und Regelungsmuster des polizeilichen Eingriffsrechts, in: Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 7. Aufl. München 2021.

Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 7. Aufl., München 2021.

Bäumler, Helmut/Mutius, Albert von (Hrsg.), Datenschutzgesetze der dritten Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts, Neuwied 1999.

Beckermann, Benedikt, Verantwortlichkeitsnormen als "Allgemeines Ordnungsrecht", DÖV 2020, 144–151.

Behr, Bernd, Shariff: Social-Media-Buttons mit Datenschutz, https://www.heise.de/hintergrund/Ein-Shariff-fuer-mehr-Datenschutz-2467514.html, Stand: 27.11.2014, zuletzt abgerufen: 17.07.2024.

Blazy, Stephan, § 5 Pflichten des Verantwortlichen I. Verantwortung für die Datenverarbeitung, in: Roßnagel, Alexander (Hrsg.), Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze. Baden-Baden 2018, 155–163.

Bock, Kirsten, Wenn die Blumenhändlerin für Facebook haftet: Die Fanpage-Entscheidung des EuGH, K&R 2019, 30–33.

Bogdandy, Armin von/Cassese, Sabino/Huber, Peter M. (Hrsg.), Band V Verwaltungsrecht in Europa: Grundzüge, Heidelberg 2014.

Born, Tobias, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, Frankfurt am Main 2014.

Brüggemann, Sebastian, Anmerkung zu EUGH: Facebook: Gemeinsame Verantwortlichkeit für Facebook-Fanpage, CR 2018, 581–582.

Brühann, Ulf, 2.4 Europarechtliche Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 131–155.

–, Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem: Zur Rechtsprechung des Europäischen Gerichtshofs, DuD[28] (2004), 201–209.

Brühann, Ulf/Zerdick, Thomas, Umsetzung der EG-Datenschutzrichtlinie, CR 1996, 429–436.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

Bull, Hans Peter, Datenschutz als Informationsrecht und Gefahrenabwehr, NJW[32] (1979), 1177–1182.

Bundesregierung, Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtver- sicherungsgesetzes – Gesetz zum autonomen Fahren, https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile, Stand: 08.02.2021, zuletzt abgerufen: 17.07.2024.

Burkert, Herbert, 2.3 Internationale Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 85–130.

Calliess, Christian/Ruffert, Matthias (Hrsg.), EUV, AEUV: Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, München, [6]2022 (zitiert: Callies/Ruffert).

Caspar, Johannes, The CJEU Google Spain Decision: Applicability of National Data Protection Law and Consequences for the EU-Data Protection Regulation, DuD 2015, 589–592.

Cimina, Veronique, The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725, ERA Forum 2020.

Cornelius, Kai, Die „datenschutzrechtliche Einheit" als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DSGVO, NZWiSt 2016, 421–426.

Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

–, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 2018.

Dammann, Ulrich, Das neue Bundesdatenschutzgesetz, NVwZ 1991, 640–643.

Dammann, Ulrich/Simitis, Spiros (Hrsg.), EG-Datenschutzrichtlinie: Kommentar, Baden-Baden, 1997 (zitiert: Dammann/Simitis DSRL).

Datenschutzkonferenz, Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO: Kurzpapier Nr. 16 2018.

Deutscher Bundestag, Drucksache 18/11534 – Entwurf eines ... Gesetzes zur Änderung des Straßenverkehrsgesetzes – Drucksache 18/11300 –, https://dserver.bundestag.de/btd/18/115/1811534.pdf, Stand: 15.03.2017, zuletzt abgerufen: 17.07.2024.

Deutscher Bundestag, Referat Öffentlichkeitsarbeit (Hrsg.), Fortentwicklung der Datenverarbeitung und des Datenschutzes: Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 19. und 23. Juni 1989, Bonn 1990.

Dovas, Maria-Urania, Joint Controllership - Möglichkeiten oder Risiken der Datennutzung: Regelung der gemeinsamen datenschutzrechtlichen Verantwortlichkeit in der DS-GVO, ZD 2016, 512–517.

Ehlers, Dirk, § 1 Wirtschaft als Gegenstand des öffentlichen Rechts, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 1 Öffentliches Wirtschaftsrecht, 4. Aufl. Heidelberg 2019, 1–49.

Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, 3. Aufl., Heidelberg 2013.

– (Hrsg.), Besonderes Verwaltungsrecht - Band 1 Öffentliches Wirtschaftsrecht, 4. Aufl., Heidelberg 2019.

– (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, 4. Aufl., Heidelberg 2020.

– (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, 4. Aufl., Heidelberg 2021.

Ehmann, Eugen/Helfrich, Marcus (Hrsg.), EG-Datenschutzrichtlinie: Kurzkommentar, Köln, 1999 (zitiert: Ehmann/Helfrich DSRL).

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO: Datenschutz-Grundverordnung, München, [2]2018 (zitiert: Ehmann/Selmayr).

– (Hrsg.), DS-GVO: Datenschutz-Grundverordnung, München, [3]2024 (zitiert: Ehmann/Selmayr).

Eickelpasch, Jörg, Die zweite Stufe der Anpassung des Datenschutzrechts des Bundes an die EU-Datenschutz-Grundverordnung, RdV 2017, 219–221.

Eller, Klaas Hendrik, Das Recht der Verantwortungsgesellschaft: Verantwortungskonzeptionen zwischen Recht, Moral- und Gesellschaftstheorie, RW 2019, 5–33.

Erbguth, Wilfried/Mann, Thomas/Schubert, Mathias, Besonderes Verwaltungsrecht: Kommunalrecht, Polizei- und Ordnungsrecht, Baurecht, 13. Aufl., Heidelberg 2019.

Eßer, Martin/Kramer, Philipp/Lewinski, Kai von (Hrsg.), DSGVO - BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze, Köln, [8]2023 (zitiert: Auernhammer).

Europäische Kommission, Commission Staff Working Document: Accompanying the document Communication From The Commission To The European Parliament And The Council - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brüssel 2020.

–, Mitteilung der Kommission an das Europäische Parlament und den Rat: Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, Brüssel 2020.

European Data Protection Board, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte: Version 2.0 2020.

–, Guidelines 8/2020 on the targeting of social media users: Version 2.0 2021.

–, Guidelines 07/2020 on the concepts of controller and processor in the GDPR: Version 2.0 2021.

European Data Protection Supervisor, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, Brüssel 2019.

Faust, Sebastian/Spittka, Jan/Wybitul, Tim, Milliardenbußgelder nach der DS-GVO?: Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, 120–125.

Folkerts, Elena, Gemeinsame Verantwortlichkeit: Grenzen der Aufteilung datenschutzrechtlicher Verpflichtungen: Anforderungen an die Gestaltung von Vereinbarungen zwischen gemeinsam Verantwortlichen, ZD 2022, 201–206.

Fritzsche, Saskia/Martini, Mario, Mitverantwortung in sozialen Netzwerken: Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra[34] (2015), 1–16.

Gierschmann, Sibylle, Gemeinsame Verantwortlichkeit in der Praxis: Systematische Vorgehensweise zur Bewertung und Festlegung, ZD 2020, 69–73.

Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln, 2018 (zitiert: G/S/S/V).

Gola, Peter (Hrsg.), DS-GVO: Datenschutz-Grundverordnung VO (EU) 2016/679, München, [2]2018 (zitiert: Gola).

Gola, Peter/Heckmann, Dirk (Hrsg.), DS-GVO: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, München, [3]2022 (zitiert: Gola/Heckmann).

Golland, Alexander, Der räumliche Anwendungsbereich der DS-GVO, DuD 2018, 351–357.

–, Reichweite des "Joint Controllership": Neue Fragen der gemeinsamen Verantwortlichkeit: Zugleich Kommentar zu EuGH, Urteil vom 29.7.2019 - C-40/17, K&R 2019, 533–537.

–, Die "private" Datenverarbeitung im Internet: Verantwortlichkeiten und Rechtmäßigkeit bei Nutzung von Plattformdiensten durch natürliche Personen, ZD 2020, 397–403.

Grafenstein, Maximilian von, The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation, Baden-Baden 2018.

Grages, Jan-Michael, Haftung und Innenausgleich in Datenschutzverträgen: Möglichkeiten zum Justieren der gesetzlichen Risikozuweisungen, CR 2020, 232–239.

–, Verarbeitung besonderer Datenkategorien: Erhöhte Anforderungen nur bei Auswertungsabsicht, https://www.cr-online.de/blog/2020/11/09/verarbeitung-besonderer-datenkategorien-erhoehte-anforderungen-nur-bei-auswertungsabsicht/, Stand: 09.11.2020, zuletzt abgerufen: 17.07.2024.

Graulich, Kurt, E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 7. Aufl. München 2021.

Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.), Europäisches Unionsrecht: Vertrag über die Europäische Union - Vertrag über die Arbeitsweise der Europäischen Union - Charta der Grundrechte der Europäischen Union, Baden-Baden, [7]2015 (zitiert: Groeben, von der/Schwarze).

Grüneberg, Christian (Hrsg.), Bürgerliches Gesetzbuch: mit Nebengesetzen insbesondere mit Einführungsgesetz (Auszug) einschließlich Rom I-, Rom II- und Rom III-Verordnungen sowie EU-Güterrechtsverordnungen, Haager Unterhaltsprotokoll und EU-Erbrechtsverordnung, Allgemeines Gleichbehandlungsgesetz (Auszug), Wohn- und Betreuungsvertragsgesetz (GrünHome), Unterlassungsklagengesetz (GrünHome), Produkthaftungsgesetz, Erbbaurechtsgesetz, Wohnungseigentumsgesetz, Versorgungsausgleichsgesetz, Lebenspartnerschaftsgesetz (GrünHome), Gewaltschutzgesetz, München, [83]2024 (zitiert: Grüneberg).

Gsell, Beate/Schellhase, Hans Martin, Vollharmonisiertes Verbraucherkreditrecht: Ein Vorbild für die weitere Angleichung des Verbrauchervertragsrechts, JZ 2009, 20–29.

Hacker, Philipp, Mehrstufige Informationsanbieterverhältnisse zwischen Datenschutz und Störerhaftung: Gestufte Kontrolle - gemeinsame Verantwortung, MMR 2018, 779–781.

Halim, Valentino/Marosi, Johannes, Status Quo der EuGH-Rechtsprechung zu Personenbezug und gemeinsamer Verantwortlichkeit: Wenig neu macht der März - Zugleich Urteilsanmerkung zu EuGH v. 7.3.2024 - C-604/22 - IAB Europe, CR 2024, 297–304.

Hanloser, Stefan, Keine gemeinsame Verantwortlichkeit für Datenspeicherung durch Facebook - Fashion ID, ZD 2019, 455–460.

Heberlein, Horst, Konkordanz der Grundrechte - multipler Grundrechtsschutz durch die Datenschutz-Grundverordnung, DVBl[135] (2020), 1225–1296.

Hense, Peter, Verantwortung für arbeitsteiliges Handeln an der Schnittstelle von Zivil-, Straf-, Wettbewerbs- und Datenschutzrecht, DSB[44] (2020), 236–238.

Hessel, Stefan/Leicht, Maximilian, Datenschutzrechtliche Verantwortlichkeit in der Forschung: Zum Spannungsverhältnis zwischen der Forschungsfreiheit und der DSGVO, DuD 2022, 305–309.

Hessel, Stefan/Potel, Karin, Catch Me If You Can - Die Widersprüche der DSGVO bei Verantwortlichkeit und Bußgeldbemessung im Konzernkontext, K&R 2020, 654–658.

Hoffmann-Riem, Wolfgang, Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer, Ludwig/Micklitz, Hans-W./Tonner, Klaus (Hrsg.), Law and diffuse Interests in the European Legal Order: Liber amicorum Norbert Reich. Baden-Baden 1997, 777–788.

Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts: Band I - Methoden Aufgaben Organisation, 2. Aufl., München 2012.

– (Hrsg.), Grundlagen des Verwaltungsrechts: Band II - Informationsordnung Verwaltungsverfahren Handlungsformen, 2. Aufl., München 2012.

– (Hrsg.), Grundlagen des Verwaltungsrechts: Band III - Personal Finanzen Kontrolle Sanktionen Staatliche Einstandspflichten, 2. Aufl., München 2013.

Hondius, Frits Willem, Emerging data protection in Europe, Amsterdam 1975.

Hustinx, Peter, Postal address: rue Wiertz 60 - B-1047 Brussels Offices: rue Montoyer 63 E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu Tel.: 02-283 19 00 - Fax : 02-283 19 50 Opinion of the European Data Protection Supervisor on the data protection reform package, https://www.edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf, Stand: 07.03.2012, zuletzt abgerufen: 17.07.2024.

Jay, Rosemary, 15. Complaints and Judicial Remedies, in: Jay, Rosemary (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition). London 2017, 283–298.

–, 17. Administrative Fines and Penalties, in: Jay, Rosemary (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition). London 2017, 315–332.

–, 9. Accountability, in: Jay, Rosemary (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition). London 2017, 169–191.

– (Hrsg.), Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice (4th edition), London 2017.

Jung, Alexander/Hansch, Guido, Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen: Hinweis zur Umsetzung im Konzern- oder Unternehmensumfeld, ZD 2019, 143–148.

Kaiser, Anna-Bettina, § 41 Bauordnungsrecht, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 2 Planungs-, Bau- und Straßenrecht, Umweltrecht, Gesundheitsrecht, Medien- und Informationsrecht, 4. Aufl. Heidelberg 2020, 210–315.

Kartheuser, Ingemar/Nabulsi, Selma, Abgrenzungsfragen bei gemeinsam Verantwortlichen: Kritische Analyse der Voraussetzungen nach Art. 26 DS-GVO, MMR 2018, 717–721.

Keller, Daphne, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, BTLJ[33] (2018), 287–364.

Kienle, Thomas, Datenmündigkeit: Zur Rechtsstellung von Kindern in der Datenschutz-Grundverordnung, PinG 2020, 208–214.

Kingreen, Thorsten/Poscher, Ralf, Polizei- und Ordnungsrecht: Mit Versammlungsrecht, 12. Aufl., München 2022.

Klement, Jan Henrik, Verantwortung: Funktion und Legitimation eines Begriffs im Öffentlichen Recht, Tübingen 2006.

Kollmar, Frederike, Umfang und Reichweite gemeinsamer Verantwortlichkeit im Datenschutz, NVwZ 2019, 1740–1743.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Ein modernes Datenschutzrecht für das 21. Jahrhundert: Eckpunkte, Stuttgart 2010.

Korff, Douwe, EC Study on Implementation of Data Protection Directive 95/46/EC, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667, Stand: 24.10.2008, zuletzt abgerufen: 17.07.2024.

Kosmider, Thomas, Die Verantwortlichkeit im Datenschutz: Die Zuordnung zum Verantwortlichen und deren Bedeutung für Rechtfertigung, Geldbußen und Schadensersatz, Stuttgart 2021.

Krämer, Ludwig/Micklitz, Hans-W./Tonner, Klaus (Hrsg.), Law and diffuse Interests in the European Legal Order: Liber amicorum Norbert Reich, Baden-Baden 1997.

Kremer, Sascha, BGH: Access-Provider sind störende Nichtstörer, https://www.cr-online.de/blog/2016/02/16/bgh-access-provider-sind-stoerende-nichtstoerer/, Stand: 16.02.2016, zuletzt abgerufen: 17.07.2024.

–, Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung?: Analyse der tatsächlichen Lebenssachverhalte zur Abgrenzung zwischen gemeinsamer Verantwortlichkeit und Auftragsverarbeitung, CR 2019, 225–234.

–, Plugins nach dem EuGH: Cookie Consent und Joint Controller überall?: Warum und wie Plugins und Tools für Websites und andere Telemedien ab sofort auf technischer Ebene zu filetieren sind, CR 2019, 676–688.

Krempl, Stefan, Datenschützer: Windows-10-Nutzer bei Telemetrie nicht aus dem Schneider, https://www.heise.de/news/Datenschuetzer-Windows-10-Nutzer-bei-Telemetrie-nicht-aus-dem-Schneider-4976556.html, Stand: 01.12.2020, zuletzt abgerufen: 17.07.2024.

Kring, Markus, Big Data und der Grundsatz der Zweckbindung im Datenschutzrecht, Frankfurt am Main 2019.

Krohm, Niclas, Die wirtschaftliche Einheit als Bußgeldadressat unter der Datenschutz-Grundverordnung?, RdV 2017, 221–226.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), DS-GVO BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, München, [4]2024 (zitiert: Kühling/Buchner).

Kuner, Christopher/Bygrave, Lee A./Docksey, Christopher/Drechsler, Laura (Hrsg.), The EU General Data Protection Regulation (GDPR): A commentary, Oxford, 2020 (zitiert: Kuner/Bygrave/Docksey).

Lachenmann, Matthias, Datenübermittlung im Konzern, Edewecht 2016.

Lauber-Rönsberg, Anne, Zum Verhältnis von Datenschutzrecht und zivilrechtlichem Äußerungsrecht, AfP 2019, 373–383.

Lee, Laureen/Cross, Samuel, (Gemeinsame) Verantwortlichkeit beim Einsatz von Drittinhalten auf Websites: Wird das Rad unnötig neu erfunden?, MMR 2019, 559–563.

Leible, Stefan (Hrsg.), Der Schutz der Persönlichkeit im Internet, Stuttgart 2012.

Lennartz, Hans-Albert, Probleme der Techniksteuerung durch Recht - am Beispiel des bundesdeutschen Datenschutzrechts: B) Teil 2, RdV 1990, 25–30.

Lepper, Ulrich/Wilde, Christian Peter, Unabhängigkeit der Datenschutzkontrolle: Zur Rechtslage im Bereich der Privatwirtschaft, CR 1997, 703–707.

Lewinski, Kai von, Formelles und informelles Handeln der datenschutzrechtlichen Aufsichtsbehörden, RdV 2001, 275–281.

Lewinski, Kai von/*Herrmann, Christoph*, Cloud vs. Cloud - Datenschutz im Binnenmarkt: Verantwortlichkeit und Zuständigkeit bei grenzüberschreitender Datenverarbeitung, ZD 2016, 467–474.

–, Vorrang des europäischen Datenschutzrechts gegenüber Verbraucherschutz- und AGB-Recht: Teil 1: Materielles Recht, PinG 2017, 165–172.

–, Vorrang des europäischen Datenschutzrechts gegenüber Verbraucherschutz- und AGB-Recht: Teil 2: Aufsichtsbehörden, PinG 2017, 209–216.

Lewinski, Kai von/*Kramer, Philipp/Eßer, Martin (Hrsg.)*, Auernhammer BDSG: Bundesdatenschutzgesetz und Nebengesetze, Köln, [4]2014 (zitiert: Auernhammer).

– (Hrsg.), DSGVO - BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze, Köln, [6]2018 (zitiert: Auernhammer, 6. Auflage).

Lezzi, Lukas/Oberlin, Jutta Sonja, Gemeinsam Verantwortliche in der konzerninternen Datenverarbeitung: Eine praxisorientierte Darstellung möglicher Konstellationen, ZD 2018, 398–404.

Lorenz, Bernd, Anonymität im Internet? - Zur Abgrenzung von Diensteanbietern und Nutzern, VuR 2014, 83–90.

Mahieu, René/van Hoboken, Joris, Fashion-ID: Introducing a phase-oriented approach to data protection?, https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/, Stand: 30.09.2019, zuletzt abgerufen: 17.07.2024.

Mahieu, René/van Hoboken, Joris/Asghari, Hadi, Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe, JIPITEC 2019, 85–105.

Mantz, Reto, Störerhaftung für Datenschutzverstöße Dritter: Sperre durch DS-RL und DS-GVO?, ZD 2014, 62–66.

Mantz, Reto/Marosi, Johannes, § 3 Vorgaben der Datenschutz-Grundverordnung, in: Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht: Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor. München 2019, 38–94.

Marosi, Johannes, Halbherzig beauftragt ist gemeinsam verantwortet: Neues aus Luxemburg zu gemeinsam Verantwortlichen, DSB 2024, 46–48.

Marx, Simon/Sütthoff, Alicia, Verantwortlichkeit auf Datenmarktplätzen: Orientierungshilfe für die Verantwortlichkeitszuweisung für einen datenschutzkonformen Handel mit personenbezogenen Daten, CR 2023, 29–35.

Masing, Johannes, Herausforderungen des Datenschutzes, NJW 2012, 2305–2311.

–, RiBVerfG Masing: Vorläufige Einschätzung der „Google-Entscheidung" des EuGH, https://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/, Stand: 14.08.2014, zuletzt abgerufen: 17.07.2024.

Mester, Britta Alexandra, Joint Control: Gemeinsame Verantwortlichkeit im Sinne der Datenschutz-Grundverordnung, DuD 2019, 167.

Mester, Britta Alexandra/Öztürk, Ebru, Joint Controllership im Unternehmensverbund: Datenschutzkonforme Umsetzung der gemeinsamen Verantwortlichkeit i.S.d. DS-GVO, DuD 2023, 73–80.

Monreal, Manfred, „Der für die Verarbeitung Verantwortliche" – das unbekannte Wesen des deutschen Datenschutzrechts: Mögliche Konsequenzen aus einem deutschen Missverständnis, ZD 2014, 611–616.

–, Die Geheimnisse der Auftragsverarbeitung, PinG 2017, 216–226.

–, Der Rahmen der Verantwortung und die klare Linie in der Rechtsprechung des EuGH zu gemeinsam Verantwortlichen: Auswirkungen der europarechtlichen Konzeption des Verantwortlichen, CR 2019, 797–808.

Moos, Flemming, Zuweisung datenschutzrechtlicher Verantwortlichkeiten in einer vernetzten Welt, in: Leible, Stefan (Hrsg.), Der Schutz der Persönlichkeit im Internet. Stuttgart 2012, 143–160.

Moos, Flemming/Rothkegel, Tobias, Gemeinsame Verantwortlichkeit eines Fanpage-Betreibers und des dazugehörigen sozialen Netzwerks: Anmerkung, MMR 2018, 596–600.

–, "Gefällt mir"-Button von Facebook - Fashion ID: Anmerkung, MMR 2019, 584–587.

Mutius, Albert von, Neuorganisation des staatlichen Datenschutzes in Schleswig-Holstein, in: Bäumler, Helmut/Mutius, Albert von (Hrsg.), Datenschutzgesetze der dritten

Generation: Texte und Materialien zur Modernisierung des Datenschutzrechts. Neuwied 1999, 92–115.

Nebel, Maxi, Datenschutzrechtliche Verantwortlichkeit bei der Nutzung von Fanpages und Social Plug-Ins, RdV 2019, 9–13.

Nebel, Maxi/Richter, Philipp, Datenschutz bei Internetdiensten nach der DS-GVO: Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2012, 407–413.

Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union: EUV/AEUV, München, [81]2024 (zitiert: Grabitz/Hilf/Nettesheim).

Nettesheim, Martin/Wolf, Manfred (Hrsg.), Das Recht der Europäischen Union: Band IV Sekundärrecht - EG-Verbraucher- und Datenschutzrecht, München, [40]2009 (zitiert: Grabitz/Hilf).

Nolde, Malaika, Sanktionen nach DSGVO und BDSG-neu: Wem droht was warum?, PinG 2017, 114–121.

OECD, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, Paris.

–, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en, Stand: 12.02.2002, zuletzt abgerufen: 17.07.2024.

–, The OECD Privacy Framework 2013.

Ohly, Ansgar, EuGH: Keine „öffentliche Wiedergabe" durch Hyperlinksetzen ohne Gewinnerzielungsabsicht - GS Media/Sanoma ua (Anmerkung), GRUR 2016, 1155–1157.

Organisation for Economic Co-operation and Development, Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data 1980.

Ossenbühl, Fritz, Vorsorge als Rechtsprinzip im Gesundheits-, Arbeits- und Umweltschutz, NVwZ 1986, 161–171.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, München, [3]2021 (zitiert: Paal/Pauly).

Piltz, Carlo, Störerhaftung im Datenschutzrecht?, K&R 2014, 80–85.

–, Gesetzentwurf zum automatisierten Fahren – Datenschutzrechtlich mangelhaft, https://www.delegedata.de/2017/02/gesetzentwurf-zum-automatisierten-fahren-datenschutzrechtlich-mangelhaft/, Stand: 28.02.2017, zuletzt abgerufen: 17.07.2024.

–, Datenschutzbehörde Hamburg: Gemeinsame Verantwortlichkeit beim Einsatz von Google Analytics (in der Standardeinstellung), https://www.delegedata.de/2020/02/datenschutzbehoerde-hamburg-gemeinsame-verantwortlichkeit-beim-einsatz-von-google-analytics-in-der-standardeinstellung/, Stand: 14.02.2020, zuletzt abgerufen: 17.07.2024.

–, Der „Dritte" nach der DSGVO, https://www.delegedata.de/2020/10/der-dritte-nach-der-dsgvo/, Stand: 19.10.2020, zuletzt abgerufen: 17.07.2024.

–, Bundesinnenministerium: DSGVO-Bußgelder müssen nach den Vorgaben des deutschen OWiG verhängt werden, https://www.delegedata.de/2021/11/bundesinnenministerium-dsgvo-bussgelder-muessen-nach-den-vorgaben-des-deutschen-owig-verhaengt-werden/, Stand: 01.11.2021, zuletzt abgerufen: 17.07.2024.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG: Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, Köln, [3]2018 (zitiert: Plath).

– (Hrsg.), DSGVO/BDSG/TTDSG: Kommentar zu DSGVO, BDSG und TTDSG, Köln, [4]2023 (zitiert: Plath).

Pünder, Hermann, § 69 Polizei- und Ordnungsrecht, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, 4. Aufl. Heidelberg 2021, 447–672.

Rachor, Frederik/Roggan, Fredrik, C. Organisation der Sicherheitsbehörden und Geheimdienste in Deutschland, in: Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 7. Aufl. München 2021.

Radtke, Tristan, The Concept Of Joint Control Under The Data Protection Law Enforcement Directive 2016/680 In Contrast To The GDPR, JIPITEC[11] (2020), 242–251.

–, Gemeinsame Verantwortlichkeit unter der DSGVO: Unter besonderer Berücksichtigung von Internetsachverhalten, Baden-Baden 2021.

Reif, Yvette, Gemeinsame Verantwortung beim Lettershopverfahren - praktische Konsequenzen der EuGH-Rechtsprechung zu den "Fanpages" und "Zeugen Jehovas", RdV 2019, 30–32.

Reimer, Philipp, Verwaltungsdatenschutzrecht: Die behördliche Datenverarbeitung als Thema für das Allgemeine Verwaltungsrecht, DÖV 2018, 881–890.

Riegel, Reinhard, 8.4 Datenschutz bei den Nachrichtendiensten, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 1474–1516.

Roßnagel, Alexander, 1. Einleitung, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 1–42.

– (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

–, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71–75.

–, Datenschutzgesetzgebung - Monopol oder Vielfalt, DuD[36] (2012), 553–555.

– (Hrsg.), Beck'scher Kommentar zum Recht der Telemediendienste: Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr, München, 2013 (zitiert: BeckRTD-Komm).

– (Hrsg.), Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018.

Roßnagel, Alexander/Geminn, Christian, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht: Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. (vzbv), Kassel 2019.

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen, Modernisierung des Datenschutzrechts: Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

Ruffert, Matthias, § 22 Grundfragen der Wirtschaftsregulierung, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 1 Öffentliches Wirtschaftsrecht, 4. Aufl. Heidelberg 2019, 835–859.

Säcker, Franz Jürgen/Zwanziger, Xenia (Hrsg.), Berliner Kommentar zum Energierecht - Band 6: MsbG - Messstellenbetriebsgesetz, Frankfurt am Main, [5]2022 (zitiert: BerlKommEnR).

Sartor, Giovanni, Provider's liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?, IDPL[3] (2013), 3–12.

–, Search Engines As Controllers: Inconvenient Implications of a Questionable Classification, MJ[21] (2014), 564–575.

Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef (Hrsg.), Sicherheitsrecht des Bundes, München, [2]2019 (zitiert: Schenke/Graulich/Ruthig).

Schiedermair, Stephanie, § 48 Selbstkontrollen der Verwaltung, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts: Band III - Personal Finanzen Kontrolle Sanktionen Staatliche Einstandspflichten, 2. Aufl. München 2013, 593–664.

Schleipfer, Stefan, EuGH: Arbeitsteiliges Zusammenwirken datenschutzrechtlicher Verantwortlicher - Fashion ID (Anmerkung), CR 2019, 579–581.

Schmeling, Margret von, Datenschutz-Aufsicht: Vom Papiertiger zur Sonderordnungsbehörde: Zur Auslegung der Eingriffsermächtigung nach § 38 Abs. 5 BDSG, DuD 2002, 351–355.

Schmidt-Preuß, Matthias, Kollidierende Privatinteressen im Verwaltungsrecht: Das subjektive öffentliche Recht im multipolaren Verwaltungsrechtsverhältnis, Berlin 1992.

Schneider, Ruben, Gemeinsame Verantwortlichkeit: Entstehung, Ausgestaltung und Rechtsfolgen des Innenverhältnisses gemäß Art. 26 DSGVO, Wiesbaden 2021.

Scholz, Rupert/Herdegen, Matthias/Klein, Hans H. (Hrsg.), Grundgesetz - Kommentar, München, [103]2024 (zitiert: Dürig/Herzog/Scholz).

Schreiber, Kristina, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden: Anwendungsbereiche, Vertragsgestaltung und Folgen nicht gleichwertiger Verantwortung, ZD 2019, 55–60.

Schulze-Fielitz, Helmuth, § 12 Grundmodi der Aufgabenwahrnehmung, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts: Band I - Methoden Aufgaben Organisation, 2. Aufl. München 2012, 823–904.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), DS-GVO / BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Heidelberg, [2]2020 (zitiert: S/J/T/K).

Simitis, Spiros, Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven, CR 1987, 602–613.

– (Hrsg.), Bundesdatenschutzgesetz, Baden-Baden, [8]2014 (zitiert: Simitis).

Simitis, Spiros/Hornung, Gerrit/Spiecker Döhmann, Indra (Hrsg.), Datenschutzrecht: DSGVO mit BDSG, Baden-Baden, 2019 (zitiert: Simitis/Hornung/Spiecker).

Simon, Dieter/Weiss, Manfred (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis, Baden-Baden 2000.

Sitzungsniederschrift der öffentlichen Anhörung am 19. Juni 1989, in: Deutscher Bundestag, Referat Öffentlichkeitsarbeit (Hrsg.), Fortentwicklung der Datenverarbeitung und des Datenschutzes: Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 19. und 23. Juni 1989. Bonn 1990, 15–16.

Sloot, Bart van der, Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe, JIPITEC[6] (2015), 211–228.

Söbbing, Thomas, Joint Controllership nach Art. 26 DSGVO: Herausforderung der datenschutzrechtlichen Gestaltung, ITRB 2020, 218–222.

Sommermann, Karl-Peter, § 86 Prinzipien des Verwaltungsrechts, in: Bogdandy, Armin von/Cassese, Sabino/Huber, Peter M. (Hrsg.), Band V Verwaltungsrecht in Europa: Grundzüge. Heidelberg 2014, 863–892.

Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht: Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München 2019.

Specht-Riemenschneider, Louisa/Schneider, Ruben, Die gemeinsame Verantwortlichkeit im Datenschutzrecht: Rechtsfragen des Art. 26 DS-GVO am Beispiel "Facebook-Fanpages", MMR 2019, 503–509.

–, Stuck Half Way: The Limitation of Joint Control after Fashion ID (C-40/17), GRUR Int 2020, 159–163.

Spiecker gen. Döhmann, Indra, Anmerkung zu EuGH, Urteil v. 9.3.2010 - C-518/07 Kommission ./. Bundesrepublik Deutschland, JZ 2010, 787–791.

–, Zur Zukunft systemischer Digitalisierung - Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen: Warum für die systemische Haftung ein neues Modell erforderlich ist, CR 2016, 698–704.

Spindler, Gerald, Datenschutz- und Persönlichkeitsrechte im Internet - der Rahmen für Forschungsaufgaben und Reformbedarf, GRUR 2013, 996–1003.

–, Durchbruch für ein Recht auf Vergessen(werden)? - Die Entscheidung des EuGH in Sachen Google Spain und ihre Auswirkungen auf das Datenschutz- und Zivilrecht4, JZ[69] (2014), 981–991.

Spindler, Gerald/Schmitz, Peter/Liesching, Marc (Hrsg.), Telemediengesetz mit Netzwerkdurchsetzungsgesetz: Kommentar, München, [2]2018 (zitiert: Spindler/Schmitz).

Stentzel, Rainer, Der datenschutzrechtliche Präventionsstaat: Rechtsstaatliche Risiken der ordnungsrechtlichen Dogmatik des Datenschutzrechts im privaten Bereich, PinG 2016, 45–49.

Sydow, Gernot/Marsch, Nikolaus (Hrsg.), DS-GVO | BDSG: Datenschutz-Grundverordnung | Bundesdatenschutzgesetz - Handkommentar, Baden-Baden, [3]2022 (zitiert: Sydow/Marsch).

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Frankfurt am Main, [2]2013 (zitiert: Taeger/Gabel).

– (Hrsg.), Kommentar DSGVO - BDSG - TTDSG, Frankfurt am Main, [4]2022 (zitiert: Taeger/Gabel).

Thiel, Markus, Polizei- und Ordnungsrecht, 5. Aufl., Baden-Baden 2022.

Tinnefeld, Marie-Theres/Petri, Thomas, Völlige Unabhängigkeit der Datenschutzkontrolle: Demokratische Legitimation und unabhängige parlamentarische Kontrolle als moderne Konzeption der Gewaltenteilung, MMR 2010, 157–161.

van Hoboken, Joris, Legal space for innovative ordering: on the need to update selection intermediary liability in the EU, Int'l J. Comm. L. & Pol'y 2009, 2–21.

Voßhoff, Andrea/Hermerschmidt, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung?, PinG 2016, 56–59.

Voßkuhle, Andreas/Eifert, Martin/Möllers, Christoph (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, 3. Aufl., München 2022.

Wagner, Bernd, Disruption der Verantwortlichkeit - Private Nutzer als datenschutzrechtliche Verantwortliche im Internet of Things, ZD 2018, 307–312.

Walz, Stefan, Das neue Bundesdatenschutzgesetz: Kompromiß als Leitprinzip, CR 1991, 364–369.

–, Selbstkontrolle versus Fremdkontrolle: Konzeptwechsel im deutschen Datenschutzrecht?, in: Simon, Dieter/Weiss, Manfred (Hrsg.), Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis. Baden-Baden 2000, 455–465.

Weber, Klaus, Rechtswörterbuch, 24. Aufl., München 2022.

Wedde, Peter, 4.3 Verantwortliche Stellen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 526–545.

Wegricht, Christiane, Das Verhältnis von Eingriffsermächtigungen des Bundes-Immissionsschutzgesetzes zur polizeilichen Generalklausel, Frankfurt am Main 2008.

Weichert, Thilo, 9.5 Chipkarten, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 1948–1966.

–, Informationstechnische Arbeitsteilung und datenschutzrechtliche Verantwortung: Plädoyer für eine Mitverantwortlichkeit bei der Verarbeitung von Nutzungsdaten, ZD 2014, 605–610.

Wielsch, Dan, Funktion und Verantwortung. Zur Haftung im Netzwerk, RW 2019, 84–108.

Wißmann, Hinnerk, § 14 Grundmodi der Aufgabenwahrnehmung, in: Voßkuhle, Andreas/Eifert, Martin/Möllers, Christoph (Hrsg.), Grundlagen des Verwaltungsrechts: Band I, 3. Aufl. München 2022, 1025–1114.

Wittner, Florian Nikolas, Verantwortlichkeit in komplexen Daten-Ökosystemen: Versuch einer Weiterentwicklung des Datenschutzes im Kontext der verteilten Verarbeitungsrealität, Tübingen 2022.

Wolff, Heinrich Amadeus/Brink, Stefan/Ungern-Sternberg, Antje von (Hrsg.), BeckOK Datenschutzrecht: DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung, München, [47]2024 (zitiert: BeckOK DatenschutzR).

Würtenberger, Thomas, § 69 Polizei- und Ordnungsrecht, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht - Band 3 Kommunalrecht, Haushalts- und Abgabenrecht, Ordnungsrecht, Sozialrecht, Bildungsrecht, Recht des öffentlichen Dienstes, 3. Aufl. Heidelberg 2013, 398–556.

Zezschwitz, Friedrich von, 3.1 Konzept der normativen Zweckbegrenzung, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung. München 2003, 219–268.

digital | recht

Staat und digitale Gesellschaft

Johannes Marosi

(Gem-)Einsame Verantwortlichkeit im Datenschutzrecht

Lange Zeit war die Rollenverteilung im Datenschutzrecht klar: ein Akteur jenseits der betroffenen Person war entweder Verantwortlicher, Auftragsverarbeiter oder datenschutzrechtlich schlicht unbeachtlich. Seit der Europäische Gerichtshof aber das Konzept der gemeinsam Verantwortlichen „wiederentdeckt" hat, scheint vor allem immer mehr digitale Infrastruktur davon erfasst zu werden. Die vorliegende Arbeit nimmt diese Entwicklung zum Anlass den Verantwortlichen insgesamt in seiner Systematik, Historie, vor allem aber den Elementen seiner Definition zu analysieren. Dabei werden auch die stetig steigende Urteilsfülle des EuGH zu der (gem-)einsamen Verantwortlichkeit systematisiert sowie die Materialien der EU-Datenschutzaufsichtsgremien kritisch untersucht.