

Steffen Mäusezahl

# Grenzen der Sicherheit der Verarbeitung personenbezogener Daten

**digital | recht**

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

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

**Band 24**

*Steffen Mäusezahl*, geboren 1990, Studium des Deutschen und Europäischen Wirtschaftsrechts (LL.M.) an der Universität Siegen.

Dissertation zur Erlangung des Dr. iur. der Fakultät III – Wirtschaftswissenschaften,  
Wirtschaftsinformatik und Wirtschaftsrecht der Universität Siegen

Tag der Disputation: 09.10.2024

Erstgutachter: Univ.-Prof. Dr. *Peter Krebs*

Zweitgutachter: Univ.-Prof. Dr. *Maximilian Becker*

Amtierender Dekan: Univ.-Prof. Dr. *Marc Hassenzahl*

Bibliografische Information der Deutschen Nationalbibliothek:

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

Dieses Buch steht gleichzeitig als elektronische Version über die Webseite der Schriftenreihe: <http://digitalrecht-z.uni-trier.de/> zur Verfügung.

Dieses Werk ist unter der Creative-Commons-Lizenz vom Typ CC BY-ND 4.0 International (Namensnennung, keine Bearbeitung) lizenziert:

<https://creativecommons.org/licenses/by-nd/4.0/deed.de>

Von dieser Lizenz ausgenommen sind Abbildungen, an denen keine Rechte der Autorin/des Autors oder der UB Trier bestehen.

Umschlagsgestaltung von Monika Molin

ISBN: 9783818741891

URN: urn:nbn:de:hbz:385-2024120909

DOI: <https://doi.org/10.25353/ubtr-f174-3261-7cae>




© 2024 Steffen Mäusezahl, Freudenberg

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

 Institut für  
Recht und Digitalisierung  
Trier

*Für meine Familie*



## Vorwort

Die vorliegende Arbeit entstand während meiner Zeit als wissenschaftlicher Mitarbeiter an der Universität Siegen. Die Arbeit wurde im Wintersemester 2023/2024 von der Fakultät für Wirtschaftswissenschaften, Wirtschaftsinformatik und Wirtschaftsrecht der Universität Siegen als Dissertation angenommen. Literatur, Rechtsprechung und sonstige Nachweise befinden sich auf dem Stand von Januar 2024.

Mein Dank gilt ganz besonders meinem Doktorvater Prof. Dr. *Peter Krebs* für die fortwährende Betreuung und Unterstützung. Dabei war es maßgeblich die Tätigkeit als studentischer Mitarbeiter an seinem Lehrstuhl, die mein Interesse weckte, den Weg einer Promotion einzuschlagen und legte damit den Grundstein für diese Arbeit. Während der Betreuung ließ er mir den Freiraum, um meine Forschungsinteressen zu verfolgen und meine Ideen zu entwickeln und auszubauen. Gleichzeitig stand er mir aber jederzeit mit Rat zur Seite. Die gemeinsamen Gespräche mit ihm haben maßgeblich dabei geholfen, die Arbeit von ihrer ersten Idee bis zu ihrer finalen Fassung stetig weiterzuentwickeln.

Bei Herrn Prof. Dr. *Maximilian Becker* möchte ich mich nicht nur für die zügige Erstellung des Zweitgutachtens bedanken. Bedanken möchte ich mich auch für seine Anregungen und Hinweise, die eine wertvolle Hilfe waren.

Bei Herrn Prof. Dr. *Jörn Griebel* möchte ich mich für seine Teilnahme an meiner Disputation bedanken. Zudem gilt mein Dank auch den Herausgebern für die Aufnahme in diese Schriftenreihe und den Mitarbeitern der Universität Trier, die den Veröffentlichungsprozess begleitet und mich hierbei unterstützt haben.

Ein wesentlicher Faktor für den erfolgreichen Abschluss der Arbeit waren schließlich auch die Rahmenbedingungen.

Daher möchte ich mich bei Prof. Dr. *Peter Krebs* und Prof. Dr. *Maximilian Becker* für die Zeit an ihren Lehrstühlen bedanken. Mein Dank gilt hier aber auch den vielen wundervollen Kolleginnen und Kollegen, mit denen ich zusammenarbeiten durfte. Die angenehme Atmosphäre und den kollegialen, zum Teil auch freundschaftlichen, Zusammenhalt und Austausch habe ich sehr hoch geschätzt. Die gemeinsame Zeit hat mir daher nicht nur sehr viel Freude bereitet. Gleichzeitig waren meine Kolleginnen und Kollegen für mich auch eine große Quelle der Motivation und eine wichtige Stütze.

Die Zeit als wissenschaftlicher Mitarbeiter hat mich sowohl fachlich als auch persönlich stark geprägt und ich werde sie und die Menschen, die mich begleitet haben, immer in guter Erinnerung behalten.

Abschließend möchte ich mich bei meiner Familie und meinen Freunden für ihre anhaltende Unterstützung und ihren Rückhalt bedanken. Ein besonderer Dank gilt dabei meinen Eltern, die mir mit ihrer uneingeschränkten Unterstützung erst die Möglichkeit gegeben haben, meinen Weg im Leben zu finden.

Freudenberg, Oktober 2024

Steffen Mäusezahl

# Inhaltsverzeichnis

Vorwort .....	V
Inhaltsverzeichnis .....	VII
Abkürzungsverzeichnis .....	XVII
Abbildungsverzeichnis .....	XXIII
Einleitung .....	1

## *Teil 1*

<i>Datenverarbeitende TOM im Spannungsverhältnis der Datenschutz-Grundverordnung .....</i>	<i>9</i>
--------------------------------------------------------------------------------------------	----------

## *Kapitel 1*

<i>Der Begriff datenverarbeitende TOM .....</i>	<i>11</i>
A. Die Bedeutung des Begriffs für die Arbeit .....	11
B. Definition .....	11

## *Kapitel 2*

<i>Datenverarbeitende TOM im Regelungsbereich zwischen Art. 32 und Art. 6 DS-GVO .....</i>	<i>15</i>
A. Begründung eines Spannungsverhältnisses zwischen Art. 32 und Art. 6 DS-GVO .....	15
I. Die Implementierung von (datenverarbeitenden) TOM nach Art. 32 DS-GVO .....	15
II. Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO .....	16
III. Konflikt zwischen Art. 32 DS-GVO und Art. 6 DS-GVO .....	19
B. Risiken aus dem Spannungsverhältnis .....	19
I. Allgemeines Haftungsrisiko .....	20
II. Gefahren für den Datenschutz .....	21

1. Gefahren für die – nach Art. 32 DS-GVO zu schützenden – betroffenen Personen.....	21
2. Gefahren für die – von den TOM – betroffenen Personen .....	22
III. Zwischenergebnis.....	24
C. Die Bedeutung datenverarbeitender TOM .....	24
I. Das Spannungsverhältnis bei datenverarbeitenden TOM in der aktuellen Diskussion .....	24
II. „Überwachungsmaßnahmen“ als Anwendungsfeld datenverarbeitender TOM .....	28
1. Allgemeines .....	28
2. Rollenkonzepte und Authentifizierungen .....	29
3. Logfiles und andere Dokumentationen .....	32
4. Daten-Backups .....	33
5. Überwachung von Datenkanälen.....	34
III. Zwischenergebnis.....	38

### *Kapitel 3*

<i>Gang der Darstellung</i> .....	39
A. Probleme und Ziele der Arbeit.....	39
B. Abgeleitete Forschungsfragen .....	41
C. Themeneingrenzung .....	42
I. Betrachtung des Gesamtproblems.....	42
II. Beschränkung auf den unternehmerischen Bereich .....	42
III. Beschränkung auf die Datenschutz-Grundverordnung .....	43
IV. Beschränkung auf den Pflichtbereich der Sicherheit der Verarbeitung .....	44
V. Beschränkung auf die Rechtmäßigkeit der Verarbeitung nach Art. 6 DS-GVO .....	45

### *Teil 2*

<i>Datenverarbeitende TOM im Lichte der Sicherheit der Verarbeitung</i> .....	49
-------------------------------------------------------------------------------	----

### *Kapitel 4*

<i>Das allgemeine Regelungsziel des Art. 32 DS-GVO</i> .....	51
A. Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.....	51



B. Schutz der Rechte und Freiheiten .....	57
I. Der Begriff des „Schutzniveaus“ .....	57
II. Risiko für die Rechte und Freiheiten (natürlicher) Personen .....	62
C. <i>Personal data breaches</i> (und andere Sicherheitsvorfälle) .....	63
I. Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO .....	63
II. Die Bedeutung des Begriffs „personal data breach“ .....	72
III. Anwendung auf (andere) Sicherheitsvorfälle .....	77
D. Einschränkung auf das Risiko für betroffene Personen .....	80
E. Das Verhältnis zu Art. 32 Abs. 4 DS-GVO .....	89
I. Überschneidungen im Anwendungsbereich .....	89
II. Probleme bei gleichrangiger Verpflichtung .....	90
F. Zwischenergebnis und grafische Darstellung .....	97

## *Kapitel 5*

<i>Anforderungen an die Sicherheit</i> .....	99
A. Risikobewertung .....	99
B. Angemessenheit des Schutzniveaus .....	101
I. Bedeutung der Angemessenheit .....	101
II. Bestimmung der Angemessenheit nach Art. 32 Abs. 2 DS-GVO ..	104
1. Die offenen Aufzählungen des Art. 32 Abs. 2 DS-GVO .....	104
2. Hinweise zur Konkretisierung der Aufzählungen in den Erwägungsgründen .....	106
3. Systematisierung des Art. 32 Abs. 2 DS-GVO .....	107
III. Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit? .....	109
1. Problem des Bezugspunkts der Kriterien .....	111
2. Wortlaut .....	113
3. Historische Auslegung .....	114
4. Systematik und Telos .....	116
5. Eigene Lösung .....	117
IV. Zwischenergebnis .....	117
C. Technische und organisatorische Maßnahmen .....	118
I. Allgemeines .....	118
II. Technischer und organisatorischer Art .....	120
III. Geeignetheit der Maßnahmen .....	124
1. Divergierende Begriffe .....	124

2. Maßnahmen als Mittel zum Zweck .....	125
3. Die „Geeignetheit“ als Einschränkung? .....	126
IV. Anforderungen an die Maßnahmen nach Art. 32 Abs. 1 Hs. 2 DS-GVO .....	127
1. Relativierung des „Verbindlichkeitsgrads“? .....	128
2. Überblick über die inhaltlichen Vorgaben .....	129
a) Pseudonymisierung und Verschlüsselung (lit. a)) .....	130
b) Fähigkeit zur Gewährleistung der Ziele: Vertraulichkeit, Integrität, Verfügbarkeit (und Belastbarkeit) (lit. b) und c)) .....	134
c) Überprüfungsverfahren (lit. d)) .....	135
3. Art. 32 Abs. 1 Hs. 2 DS-GVO als unverbindliche Orientierungshilfe .....	136
V. Telos als Basis gesetzgeberischer Vorgaben .....	138
1. Gefahr des Widerspruchs zwischen Vorgaben und Ziel .....	138
2. Vorgaben unter Berücksichtigung der Einzelfallprüfung .....	141
3. Zielorientierte Pflicht .....	141
VI. Zwischenergebnis .....	142

## Kapitel 6

<i>Wesentliche Ergebnisse für die Problemstellung</i> .....	143
A. Der Regelungsinhalt von Art. 32 DS-GVO unter Beachtung des Problems datenverarbeitender TOM .....	143
I. Pflicht zur Gewährleistung eines angemessenen Schutzniveaus .....	143
II. Keine Pflicht zur Implementierung (datenverarbeitender) TOM ..	144
B. Abgleich der bisherigen Erkenntnisse mit der Arbeitshypothese .....	145
C. Überarbeitung der Arbeitshypothese .....	147
I. „Pflicht“ zur Implementierung bestimmter (datenverarbeitender) TOM .....	147
1. „Zwingende“ Maßnahmen für die Gewährleistung des angemessenen Schutzniveaus .....	147
2. Datenverarbeitende TOM als zwingende Maßnahmengruppe ...	148
II. Anordnung von Sicherheitsmaßnahmen durch Aufsichtsbehörden .....	149
III. Gefahr einer Verzerrung der Angemessenheit .....	150
D. Schlussfolgerung .....	151

*Kapitel 7*

<i>Berücksichtigung datenverarbeitender TOM</i> .....	153
A. Überlegungen zur Berücksichtigung datenverarbeitender TOM .....	153
I. Zwingende Differenzierung zwischen Sicherheit und Sicherheitsmaßnahmen .....	153
II. Datenverarbeitende TOM als Teil der Angemessenheitsprüfung ..	154
III. Die datenschutzrechtliche Bewertung von Sicherheitsmaß- nahmen .....	155
B. Subsumtion unter die Abwägungskriterien des Art. 32 Abs. 1 DS-GVO	156
I. Stand der Technik .....	156
II. Implementierungskosten .....	160
III. Verarbeitungskriterium .....	162
IV. Risiko für die Rechte und Freiheiten betroffener Personen .....	164
1. Allgemeines .....	164
2. Möglichkeit einer Doppelfunktion .....	164
V. Systematisierung und Zwischenergebnis .....	166
C. Die datenschutzrechtliche Bewertung von TOM als ungeschriebenes Tatbestandsmerkmal der Abwägung .....	168
I. Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO .....	168
1. Die datenschutzrechtliche Bewertung als Aufrechterhaltung einer widerspruchsfreien Rechtsordnung .....	168
2. Die Berücksichtigung einzelner Sicherheitsmaßnahmen im jetzigen System der Abwägung .....	170
3. Die teleologische Rechtfertigung für ein eigenes Abwägungskriterium .....	171
4. Zwischenergebnis .....	175
II. Methodische Begründung .....	175
1. Darstellung möglicher Lösungswege .....	175
2. Abschließende oder offene Aufzählung der Abwägungskrite- rien .....	179
a) Grundlage .....	179
b) Offene Aufzählung der (inneren) zweiten Ebene .....	180
c) Offene Aufzählung der (äußeren) ersten Ebene .....	182
aa) Grundlagen .....	182

- bb) Die erste Aufzählung des Art. 32 Abs. 2 DS-GVO als echte, offene Aufzählung ..... 182
- cc) Systematische Widersprüche? ..... 185
- dd) Doch unterschiedliche Bezugspunkte der Kriterien? ..... 186
- ee) Eigene Lösung ..... 187
- d) Zwischenergebnis und „Neugliederung“ von Art. 32 DS-GVO ..... 187
- 3. Die datenschutzrechtliche Bewertung von TOM als unbenannter Abwägungstatbestand durch Auslegung der offenen Aufzählung ..... 190
- 4. Alternative: Die datenschutzrechtliche Bewertung von TOM als unbenannter Abwägungstatbestand im Wege einer teleologischen Reduktion ..... 193
- III. Konkretisierung des ungeschriebenen Abwägungskriteriums der datenschutzrechtlichen Bewertung von TOM ..... 195
- D. Zwischenergebnis ..... 198

*Teil 3*

- Die Rechtmäßigkeit datenverarbeitender TOM ..... 201*

*Kapitel 8*

- Das System der Rechtmäßigkeit von Datenverarbeitungen ..... 203*
- A. Die Notwendigkeit einer Rechtsgrundlage ..... 203
- B. Ausrichtung am Zweck der Verarbeitung ..... 205
  - I. Zweck der Verarbeitung ..... 205
  - II. Der Zweck innerhalb der Rechtsgrundlagen ..... 208
  - III. Zwischenergebnis ..... 213
- C. Der Legitimationsgedanke hinter den Rechtsgrundlagen ..... 213
  - I. Die Aufteilung in Einwilligung und gesetzliche Rechtsgrundlagen 213
  - II. Die Selbstbestimmung der betroffenen Person als Legitimation... 216
  - III. Die gesetzlichen Rechtsgrundlagen als vordefinierte Eingriffsrechtfertigung ..... 221
    - 1. Die gesetzlichen Rechtsgrundlagen als Ausdruck einer Grundrechtsabwägung ..... 221
    - 2. Verwirklichung der Abwägung ..... 223
      - a) Vollkommene Rechtsgrundlagen ..... 224
      - b) Ergänzungsbedürftige Rechtsgrundlagen ..... 225

c) Abwägende Rechtsgrundlage .....	227
d) Grafische Zusammenfassung .....	231
3. Zwischenergebnis .....	233
IV. Zwischenergebnis.....	233
D. Schlussfolgerung .....	234

### *Kapitel 9*

<i>Rechtsgrundlage für datenverarbeitende TOM</i> .....	237
A. Die Sicherheit der Verarbeitung als Verarbeitungszweck? .....	237
B. Art. 32 DS-GVO als ergänzende Rechtsgrundlage .....	240
I. „Verpflichtung“ zur Verarbeitung personenbezogener Daten nach Art. 32 DS-GVO .....	240
II. Anforderungen an den Zweck der Verarbeitung .....	243
C. Die Frage einschlägiger Rechtsgrundlagen .....	247
I. Anforderungen an die „Auswahl“ einer geeigneten Rechtsgrund- lage .....	247
II. Schlussfolgerungen und denkbare Rechtsgrundlagen für datenverarbeitende TOM .....	251
III. Die Untauglichkeit der Einwilligung .....	253
1. Rechtsunsicherheit über die Zustimmung .....	253
2. Widerrufsrecht .....	255
3. Berücksichtigung im Rahmen des Art. 32 DS-GVO? .....	257
a) Verweigerung oder Widerruf der Einwilligung als Verzicht auf den Schutz nach Art. 32 DS-GVO .....	257
b) Allgemeine Berücksichtigung im Rahmen der Angemessenheitsprüfung ...	258
c) Praktische Probleme .....	259
4. Denkbare Anwendungsfälle und Zwischenergebnis.....	260
IV. Das Widerspruchsrecht als Ausschlussgrund für gesetzliche Rechtsgrundlagen .....	262
D. Zwischenergebnis.....	265

### *Kapitel 10*

<i>Der Tatbestand der Erforderlichkeit</i> .....	267
A. Der Tatbestand im System der Rechtsgrundlagen .....	267
B. Bezugspunkte des Tatbestands .....	269
I. Die Erforderlichkeit als Bindeglied.....	269

II. Die Datenverarbeitung als erster Bezugspunkt.....	270
III. Der Zweck als zweiter Bezugspunkt .....	271
1. Zweckrahmen der Rechtsgrundlage oder Zweck der Verarbeitung .....	271
2. Ermittlung des zweiten Bezugspunkts im Wege der Auslegung..	272
a) Sprachliche Anknüpfung.....	273
b) Die Systematik des Tatbestands .....	274
c) Teleologische Erwägungen .....	275
IV. Zwischenergebnis.....	276
C. Autonome, übergreifende Auslegung .....	277
I. Allgemeines.....	277
II. Der Grundsatz europäisch autonomer Auslegung und der Verweis auf u.a. das nationale Recht .....	278
III. Differenzierung zwischen Auslegungsmaßstab und Auslegungsergebnis.....	283
IV. Zwischenergebnis.....	286
D. Auslegung der Erforderlichkeit.....	286
I. Denkbare Bewertungsmaßstäbe .....	287
1. Alternativen zur Datenverarbeitung.....	287
2. Qualifizierung der Zweckerreichung.....	288
3. Verhältnis zwischen Datenverarbeitung und Zweck .....	291
II. Eigene Auslegung .....	292
1. Wortlaut .....	292
2. Systematik .....	294
3. Telos .....	294
III. Würdigung der Bewertungsmaßstäbe und eigene Lösung .....	297
IV. Zwischenergebnis.....	299
E. Folgen für das Problem datenverarbeitender TOM .....	299
I. Einschränkung der weiteren Untersuchung .....	300
II. Wechselwirkung zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle.....	300
III. Der Auslegungsmaßstab der Erforderlichkeit als entscheidende Weichenstellung.....	301

*Teil 4*

<i>Lösungsvorschlag für das Spannungsverhältnis</i> .....	303
-----------------------------------------------------------	-----

*Kapitel 11*

<i>Methodik</i> .....	305
A. Untersuchungsergebnisse als Basis für den Lösungsansatz .....	305
B. Ansatz zur Lösung des Spannungsverhältnisses.....	307
I. Grundlage .....	307
II. Instrumente.....	307
III. Ziele eines Lösungsansatzes .....	308
1. Allgemeines .....	308
2. Die Bedeutung alternativer TOM .....	309
3. Zwischenergebnis.....	310
C. Praktische Umsetzung des Lösungsansatzes.....	311

*Kapitel 12*

<i>Prüfungsablauf</i> .....	313
A. Identifikation und Bewertung des Risikos der Verarbeitung .....	313
B. Bestandsaufnahme geeigneter TOM.....	318
C. Bewertung der TOM .....	321
D. Festlegung einer „Implementierungsreihenfolge“ .....	322
E. Ableitung des angemessenen Schutzniveaus .....	324
F. Überprüfung des angemessenen Schutzniveaus.....	326

*Kapitel 13*

<i>Darstellung anhand eines Beispiels</i> .....	329
-------------------------------------------------	-----

*Kapitel 14*

<i>Übertragbarkeit der Lösung</i> .....	341
A. Datenverarbeitende TOM als Teil einer Gruppe vergleichbarer Maßnahmen .....	341
B. Von der „datenschutzrechtlichen Bewertung“ hin zur „rechtlichen Bewertung“.....	342
C. Gesonderte Beachtung der „Regulierungsvorschriften“ .....	343
D. Übertragbarkeit des Prüfungsablaufs .....	344
E. Zwischenergebnis.....	345

Schlussthesen.....	347
Literaturverzeichnis.....	357
Sonstige Quellen.....	383
Rechtsprechungsverzeichnis.....	389



## Abkürzungsverzeichnis

a.A.	andere Ansicht
a.F.	alte Fassung
A-SIT	Zentrum für sichere Informationstechnologie - Austria
Abl.	Amtsblatt
Abs.	Absatz
AcP	Archiv für die civilistische Praxis (Zeitschrift)
AER	The American Economic Review (Zeitschrift)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Alt.	Alternative
Anm.	Anmerkung
Art.	Artikel
Aufl.	Auflage
Az.	Aktenzeichen
BC	Zeitschrift für Bilanzierung, Rechnungswesen und Controlling (Zeitschrift)
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BeckRS	Beck online Rechtsprechung
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen
KA	Bundeskanzleramt [Österreich]
BKR	Bank- und Kapitalmarktrecht (Zeitschrift)
BSI	Bundesamt für Sicherheit in der Informationstechnik

bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
bzw.	beziehungsweise
CCZ	Corporate Compliance (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
Datenverarbeiter	Verantwortlicher und Auftragsverarbeiter (zusammengefasst)
DCGK	Deutscher Corporate Governance Kodex
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DS	Die Sachverständigen (Zeitschrift)
DSB	Datenschutzbehörde [Österreich]
DS-GVO/DSGVO	Datenschutz-Grundverordnung <i>(Die hier vorrangig genutzte Abkürzung ist „DS-GVO“. Die Abkürzung „DSGVO“ wird allenfalls bei einem Verweis auf andere Werke genutzt, die diese Abkürzung verwenden)</i>
DS-RL	Datenschutzrichtlinie
DSK	Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DStR	Deutsches Steuerrecht (Zeitschrift)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
ECLI	European Case Law Identifier/Europäischer Rechtsprechungs-Identifikator
Ed.	Edition
EDSA	Europäischer Datenschutzausschuss
EL	Ergänzungslieferung
EG	Europäische Gemeinschaft
Einf.	Einführung
ErwG	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EUArbRK	Kommentar zum europäischen Arbeitsrecht
EuGH	Gerichtshof der Europäischen Union
EuR	Europarecht (Zeitschrift)
EUV	Vertrag über die Europäische Union

EuZA	Europäische Zeitschrift für Arbeitsrecht (Zeitschrift)
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
EWR	Europäischer Wirtschaftsraum
EWS	Europäisches Wirtschafts- und Steuerrecht (Zeitschrift)
f.	folgend
ff.	folgende
Fn.	Fußnote
FS	Festschrift
GA	Generalanwalt
GDPR	General Data Protection Regulation (siehe auch DS-GVO)
gem.	gemäß
grds.	grundsätzlich
GRC/GrCh	Charta der Grundrechte der Europäischen Union <i>(Die hier vorrangig genutzte Abkürzung ist „GrCh“. Die Abkürzung „GRC“ wird allenfalls bei einem Verweis auf andere Werke genutzt, die diese Abkürzung verwenden)</i>
Hdb.	Handbuch
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
Hs.	Halbsatz
i.d.R.	in der Regel
i.H.v.	in Höhe von
i.S.d./e.	im Sinne des/der/eines
ICO	Information Commissioner's Office
insb.	insbesondere
InTeR	Innovations- und Technikrecht (Zeitschrift)
IoT	Internet of Things
IT	Informationstechnik/Informationstechnologie
JEI	Journal of Economic Issues
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristen Zeitung (Zeitschrift)
Kap.	Kapitel
K&R	Kommunikation und Recht (Zeitschrift)
LG	Landgericht
lit.	litera

LSG	Landessozialgericht
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift für IT-Recht und Recht der Digitalisierung)
MüKo	Münchener Kommentare
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (Zeitschrift)
p.	page
pp.	pages
PinG	Privacy in Germany (Zeitschrift)
RabelsZ	Rabels Zeitschrift für ausländisches und internationales Privatrecht (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RG	Reichsgericht
RGZ	Entscheidungssammlung des Reichsgerichts in Zivilsachen
Rn.	Randnummer
Rs.	Rechtssache
S.	Satz (bei Rechtsnormen) oder Seite (bei Quellennachweisen)
sog.	sogenannt
TOM (auch TOMs)	Technische und organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
u.a.	und andere/unter anderem
UAbs.	Unterabsatz
ugs.	umgangssprachlich
v.	von
verb.	verbunden
VG	Verwaltungsgericht
vgl.	vergleiche
Vol.	Volumen
WHG	Gesetz zur Ordnung des Wasserhaushalts

ZD	Zeitschrift für Datenschutz (Zeitschrift)
ZEuP	Zeitschrift für Europäisches Privatrecht (Zeitschrift)
ZfpW	Zeitschrift für die gesamte Privatrechtswissenschaft (Zeitschrift)
zit.	zitiert
ZphF	Zeitschrift für philosophische Forschung (Zeitschrift)
ZVertriebsR	Zeitschrift für Vertriebsrecht (Zeitschrift)



## Abbildungsverzeichnis

Abb. 1: System der Sicherheit der Verarbeitung nach Art. 32 DS-GVO (eigene Darstellung)	97
Abb. 2: Ebenen der Aufzählungen des Art. 32 Abs. 2 DS-GVO (eigene Darstellung).....	108
Abb. 3: System der benannten Abwägungskriterien zur Bestimmung des angemessenen Schutzniveaus (eigene Darstellung) .....	167
Abb. 4: Bestimmung des angemessenen Schutzniveaus (eigene, die Abb. 2 ergänzende Darstellung) .....	188
Abb. 5: Bestimmung des angemessenen Schutzniveaus unter Berücksichtigung datenverarbeitende TOM (eigene, die Abb. 2 und 4 ergänzende, aber z.T. gekürzte Darstellung) .....	192
Abb. 6: Festlegung der Verarbeitungsinteressen für die Abwägung innerhalb der gesetzlichen Rechtsgrundlagen (eigene Darstellung).....	232
Abb. 7: Verhältnis von Zweck und Zweckrahmen bei der Auswahl einer Rechtsgrundlage (eigene Darstellung).....	235
Abb. 8: Vereinfachte Darstellung einer Verarbeitung im Rahmen eines CRM-Prozesses (eigene Darstellung).....	330
Abb. 9: Zuordnung der Gefahren anhand eines Ausschnitts aus Abb. 8 (eigene Darstellung) .....	331
Abb. 10: Gegenüberstellung von Gefahren und Maßnahmen(-kategorien) (eigene Darstellung) .....	333
Abb. 11: Bewertung der technischen und organisatorischen Maßnahmen (eigene Darstellung) .....	336
Abb. 12: Reihenfolge für die Implementierung technischer und organisatorischer Maßnahmen (eigene Darstellung) .....	337





## Einleitung

Technische und organisatorische Maßnahmen (kurz: TOM oder auch TOMs)<sup>1</sup> dienen in mehreren Vorschriften der Datenschutz-Grundverordnung<sup>2</sup> (DS-GVO) der Erfüllung rechtlicher Anforderungen.<sup>3</sup> Ein Bereich ist die Sicherheit der Verarbeitung – oder häufig auch „Datensicherheit“<sup>4</sup> genannt –<sup>5</sup> nach Art. 32 DS-GVO. Gemäß Art. 32 Abs. 1 DS-GVO müssen Verantwortliche und Auftragsverarbeiter technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten. Das Ziel der Sicherheit der Verarbeitung liegt dabei in der Vermeidung von Sicherheitsvorfällen wie die unbefugte Offenlegung von oder der unbefugte Zugang zu Daten (bspw. durch Hackerangriffe)<sup>6</sup>, die unbeabsichtigte Vernichtung oder auch der Verlust von Daten (vgl. Art. 32 Abs. 2 DS-GVO).<sup>7</sup>

---

<sup>1</sup> Statt vieler zunächst DatKomm/*Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 3; Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 12; siehe auch Kap. 1, B. *Definition*.

<sup>2</sup> 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).

<sup>3</sup> Auf technische und organisatorische Maßnahmen verweisen die Art. 5 Abs. 1 lit. f), 24, 25, 28, 32, 34, 89 DS-GVO.

<sup>4</sup> Statt vieler zunächst Roßnagel/*Husemann*, Das neue Datenschutzrecht, 2018, § 5, Rn. 135; siehe auch Kap. 4, A. *Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.*

<sup>5</sup> Kritisch hierzu: Kap. 4, A. *Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.*

<sup>6</sup> Siehe zur Gefahr für die Sicherheit durch Hacker: Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 1, 35b; Plath/*Grages*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 11.

<sup>7</sup> Eine kritische Auseinandersetzung mit den Zielen der Sicherheit der Verarbeitung erfolgt in Kap. 4, C. *Personal data breaches (und andere Sicherheitsvorfälle)*.

Die Sicherheit der Verarbeitung steht dabei in einem engen Zusammenhang mit einem „personal data breach“<sup>8</sup> (ugs. häufig auch „Datenpanne“<sup>9</sup>) i.S.d. Art. 4 Nr. 12 DS-GVO, der eine Verletzung der Sicherheit darstellt.<sup>10</sup> Auch wenn ein personal data breach nicht zwangsweise einen Verstoß gegen Art. 32 DS-GVO darstellt,<sup>11</sup> stellt sich jedoch stets die Frage, ob eine unzureichende Sicherheit i.S.d. Art. 32 DS-GVO für den personal data breach ursächlich war.<sup>12</sup> Unter den Voraussetzungen des Art. 33 DS-GVO muss ein personal data breach an die zuständige Datenschutzaufsichtsbehörde gemeldet werden. Aus der Anzahl dieser Meldungen (auch sog. „personal data breach notifications“) lassen

---

<sup>8</sup> Deutsch: „Verletzung des Schutzes personenbezogener Daten“, Französisch: „violation de données à caractère personnel“, Spanisch: „violación de la seguridad de los datos personales“, Italienisch: „violazione dei dati personali“, Niederländisch: „inbreuk in verband met persoonsgegevens“.

<sup>9</sup> Weber/Eßler/Weber, Rechtswörterbuch, Stand: 31. Ed. 2023, Begriff: „Datenpanne“; Maslewski, ZD 2023, S. 251, 252; Wybitul, NJW 2020, S. 2577 ff.; Fuhrrott, NZA 2019, S. 649 ff.; Sassenberg/Faber/Mantz/Spittka, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 135; Knyrim/Zavadil, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 11.1; Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 912 f., spricht sowohl von „Datenpannen“ als auch „Sicherheitspannen“; vgl. auch Kasner, PinG 2019, S. 111 ff., Brams, ZD 2023, S. 484 ff.; Marschall, DuD 2015, S. 183 ff., auf Basis der Entwurfsfassung der Datenschutz-Grundverordnung.

<sup>10</sup> Statt vieler zunächst Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 6, siehe hierzu ausführlicher: Kap. 4, C., II. Die Bedeutung des Begriffs „personal data breach“.

<sup>11</sup> Becker, ZD 2020, S. 175, 177; Knyrim/Zavadil, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 11.11; vgl. Simitis/Hornung/Spiecker gen. Döhmann/Dix, Datenschutzrecht, 2019, Art. 4 Nr. 12 DS-GVO, Rn. 2, 4; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 12 DS-GVO, Rn. 6; Kuner/Bygrave/Docksey/Burton, GDPR, 2020, p. 637; v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 1 (siehe auch dort Fn. 1). Siehe auch EuGH, Rs. C-340/21 (Natsionalna agentsia za prihodite), ECLI:EU:C:2023:986 = BeckRS 2023, 35786, Rn. 29 ff.

<sup>12</sup> Wybitul, NJW 2020, S. 2577, Rn. 23; vgl. Ehmann/Selmayr/Klabunde, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 56; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 4 DS-GVO, Rn. 27; für eine Indizwirkung Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 31; vgl. auch Brams, ZD 2023, S. 484, 485, wonach dies „im Regelfall auf eine Verletzung der Datensicherheit nach Art. 32 DS-GVO zurückzuführen“ ist. Siehe auch EuGH, Rs. C-340/21 (Natsionalna agentsia za prihodite), ECLI:EU:C:2023:986 = BeckRS 2023, 35786, Rn. 22 ff., der einen personal data breach „allein nicht ausreichend[en]“ lässt für einen Verstoß gegen insb. Art. 32 DS-GVO (Rn. 39).

sich damit auch erste Rückschlüsse auf die praktische Bedeutung der Sicherheit der Verarbeitung ableiten. So kommt die Anwaltskanzlei DLA Piper für die Zeit seit dem 25. Mai 2018 (Geltung der Datenschutz-Grundverordnung, vgl. Art. 99 Abs. 2 DS-GVO) bis 27. Januar 2023 auf etwas über 460.000<sup>13</sup> personal data breach notifications im Europäischen Wirtschaftsraum (EWR) und dem Vereinigten Königreich.<sup>14</sup>

Bei der Vielzahl an Meldungen verwundert es daher nicht, dass gerade auch aufsehenerregende Verfahren der Aufsichtsbehörden, wie bspw. gegen 1&1<sup>15</sup> (unzureichendes Authentifizierungsverfahren für die Herausgabe von Informationen im Bereich des Kundensupports), British Airways<sup>16</sup> (unzureichender Schutz von Kundendaten, insbesondere auch Kreditkarteninformationen) und Marriott International<sup>17</sup> (unzureichender Schutz der Kundendatenbank) die Sicherheit der Verarbeitung zum Verfahrensgegenstand hatten.<sup>18</sup>

---

<sup>13</sup> Aufgrund einer unzureichenden Datenlage konnten einige Länder nicht berücksichtigt werden. Zudem kam es auch stellenweise zu Hochrechnungen, wenn Daten nur für einen Teil des Zeitraums vorlagen. Ferner könnten sich Meldungen auch noch auf die Rechtslage vor der Datenschutz-Grundverordnung beziehen. Siehe zu diesen Anmerkungen: DLA Piper, GDPR fines and data breach survey: January 2023, S. 19, Sternchenverweis.

<sup>14</sup> DLA Piper, GDPR fines and data breach survey: January 2023, S. 19, aufgeteilt nach den Ländern des EWR und dem Vereinigten Königreich.

<sup>15</sup> Ursprünglich erließ der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), als zuständige Aufsichtsbehörde, ein Bußgeld i.H.v. 9,55 Mio. Euro, BfDI, Pressemitteilung 30/19, 09.12.2019; vgl. auch LG Bonn, BeckRS 2020, 35663, Rn. 13. Das Bußgeld wurde später durch das LG Bonn auf 900.000 Euro herabgesetzt, LG Bonn, BeckRS 2020, 35663, Rn. 74; siehe auch zu diesem Verfahren *Kiparski/Zirfas*, CR 2021, S. 108 ff.

<sup>16</sup> Ursprünglich wollte das Information Commissioner's Office (ICO), als zuständige Aufsichtsbehörde, ein Bußgeld in Höhe von 183,39 Mio. Pfund verhängen, IOC, Penalty Notice, Case ref: COM0783542 British Airways plc, 16.10.2020, Rn. 5.3.; vgl. *Wybitul*, NJW 2020, S. 2577, Rn. 5, Fn. 12. Letztlich wurde ein Bußgeld von 20 Mio. Pfund festgelegt, IOC, Penalty Notice, Case ref: COM0783542 British Airways plc, 16.10.2020, Rn. 1.7., 7.123.; vgl. *Kipker*, MMR-Aktuell 2020, 433456, unter „Datenpanne bei British Airways“.

<sup>17</sup> Ursprünglich wollte das IOC ein Bußgeld i.H.v. 99,2 Mio Pfund verhängen, IOC, Penalty Notice, Case ref: COM0804337 Marriott International Inc, 30.10.2020, Rn. 5.3.; vgl. *Wybitul*, NJW 2020, S. 2577, Rn. 5, Fn. 12; *Meyer*, ZVertriebsR 2021, S. 1, 2. Verhängt wurde ein Bußgeld i.H.v. 18,4 Mio Pfund, IOC, Penalty Notice, Case ref: COM0804337 Marriott International Inc, 30.10.2020, Rn. 1.7., 7.55.; vgl. *Meyer*, ZVertriebsR 2021, S. 1, 2.

<sup>18</sup> Laut der Internetseite von CMS Law.Tax, <https://www.enforcementtracker.com> wurden EU-weit bislang 355 Bußgelder aufgrund von „*Insufficient technical and organisational measures to ensure information security*“ verhängt, die in Summe ein Bußgeld i.H.v. 385.602.875

Die Sicherheit der Verarbeitung dürfte dabei als die wertungsmäßig konsequente Fortführung der „datenschutzrechtlichen Vorabkontrolle“ anzusehen sein.<sup>19</sup> Im deutschsprachigen Raum wird sie eher mit dem Konstrukt „Verbot mit Erlaubnisvorbehalt“<sup>20</sup> klassifiziert. Das Prinzip dahinter: Für jede Verarbeitung personenbezogener Daten muss vorab eine Rechtsgrundlage bestehen, die die Verarbeitung „erlaubt“.<sup>21</sup> In der Verordnung wird dies zentral<sup>22</sup> in Art. 6 DS-GVO geregelt.

Die Vorabkontrolle und die Sicherheit der Verarbeitung regeln gemeinsam den Schutz vor den negativen Auswirkungen einer Verarbeitung personenbezo-

---

Euro ergaben. Sortiert nach Art des Verstoßes erreichen sie damit Platz 3, direkt hinter „*Insufficient legal basis for data processing*“ (Platz 2) und „*Non-compliance with general data processing principles*“ (Platz 1). Laut Angaben wurden nur Bußgelder mit gesicherten Informationen zur Höhe und Art der Verletzung berücksichtigt. Bei diesem Ranking sollte man auch nicht unberücksichtigt lassen, dass manche Aufsichtsbehörden scheinbar neben einer Verletzung spezifischer Vorschriften gleichzeitig auch teilweise das Bußgeld auf einen Verstoß gegen die Grundprinzipien stützen. (Die Daten wurden zuletzt abgerufen am 14.01.2024).

<sup>19</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27, wonach es erst einer Rechtsgrundlage nach Art. 6 DS-GVO bedarf; John/Schaller, CR 2022, S. 156, 156, wonach ein „effektiver Datenschutz“ sich aus der „Zulässigkeit der Datenverarbeitung“ und der „Sicherheit der Verarbeitung“ zusammensetzt; ähnlich Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 2, wonach es „flankierende Maßnahmen zur Datensicherheit“ braucht; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 1 f., „Neben dem Vorliegen eines Erlaubnistatbestands (Art. 6) [...] bedarf es auch eines Schutzes auf faktischer Ebene [...]“.

<sup>20</sup> Statt vieler zunächst Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 1; kritisch zu diesem Begriff BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 11; siehe hierzu ausführlicher: Kap.2, A., II. Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO.

<sup>21</sup> Statt vieler zunächst Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 4; siehe hierzu: Kap.2, A., II. Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO.

<sup>22</sup> Statt vieler zunächst Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 1; siehe auch: Kap.2, A., II. Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO. In einem engen Zusammenhang mit Art. 6 DS-GVO und dem Erfordernis einer datenschutzrechtlichen Rechtsgrundlage für die Verarbeitung stehen auch die Art. 9 f. DS-GVO und deren Verhältnis zueinander, siehe hierzu ausführlicher: Kap. 3, C., V. Beschränkung auf die Rechtmäßigkeit der Verarbeitung nach Art. 6 DS-GVO und insb. die Nachweise in Fn. 18.

gener Daten über den gesamten Verarbeitungszyklus. Die Vorabkontrolle bewertet die negativen Auswirkungen für die betroffenen Personen durch die Verarbeitung ihrer personenbezogenen Daten, um zu entscheiden, „ob“ überhaupt eine Verarbeitung stattfinden darf.<sup>23</sup> Dagegen befasst sich die Sicherheit der Verarbeitung mit den (faktischen) Gefahren während der (anschließenden) Verarbeitung und stellt daher Anforderungen an das „Wie“ personenbezogener Daten verarbeitet werden dürfen.<sup>24</sup> Ohne das Verhältnis beider Vorschriften zueinander hier klar zu definieren, entsteht der Eindruck, dass die Sicherheit der Verarbeitung auf den Wertungen der Vorabkontrolle aufbaut und beide Vorschriften in einem harmonischen Verhältnis zueinanderstehen.

Diese Annahme ist jedoch nicht ganz zutreffend. Denn verarbeiten technische und organisatorische Maßnahmen in Erfüllung des Art. 32 DS-GVO ihrerseits personenbezogene Daten (hier bezeichnet als „datenverarbeitende TOM“)<sup>25</sup> könnten beide Vorschriften in Konflikt miteinander treten. Maßnahmen, die eigentlich die Anforderungen an den Datenschutz erfüllen sollen, unterfallen dann mit ihrer zugrundeliegenden Datenverarbeitung ihrerseits der datenschutzrechtlichen Vorabkontrolle nach Art. 6 DS-GVO. Datenverarbeitende TOM begründen damit ein Spannungsverhältnis zwischen der Sicherheit der Verarbeitung nach Art. 32 DS-GVO und der datenschutzrechtlichen Vorabkontrolle nach Art. 6 DS-GVO.

---

<sup>23</sup> Vgl. hinsichtlich des Regelungsgehalts des „Ob“ eine Verarbeitung zulässig ist: Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 1; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 7; Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 3.

<sup>24</sup> Vgl. Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 1 f., zur Bedeutung eines insb. zu Art. 6 DS-GVO ergänzenden Schutzes personenbezogener Daten auf „faktischer Ebene“. Siehe ebenfalls allgemein zur Bedeutung eines faktischen Schutzes als Ergänzung rechtlicher Vorgaben: Simitis/Hornung/Spiecker gen. Döhmann/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung, Rn. 244 ff. (insb. Rn. 245); Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 5; Jandt, DuD 2017, S. 562, 562. Siehe hinsichtlich des „Wie“: Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 3, mit Verweis auf Art. 32 DS-GVO, siehe auch zur Differenzierung zwischen „Datenschutz“ und „Datensicherheit“: Seufert, ZD 2023, S. 256, 257; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 1b.

<sup>25</sup> Näher zu diesem Begriff: Kap. 1 *Der Begriff* datenverarbeitende TOM.

Überspitzt lässt sich dieses Spannungsverhältnis in der Frage darstellen:

*„Müssen Eingriffe in den Schutz vor einer Verarbeitung personenbezogener Daten hingenommen werden, um die Sicherheit der Verarbeitung (anderer) personenbezogener Daten zu gewährleisten?“*

Unzweifelhaft dürfte aus der Datenschutz-Grundverordnung abzuleiten sein, dass ein „Mehr“ an Sicherheit ein wünschenswertes Ziel darstellt.<sup>26</sup> Datenverarbeitende TOM lassen jedoch daran zweifeln, ob die Gewährleistung der Sicherheit der Verarbeitung in jedem Fall wünschenswert ist oder ob sie nicht Grenzen unterliegen sollte, wenn dies andernfalls zum Einsatz rechtlich unerwünschter, datenverarbeitender TOM führen könnte. Auf den ersten Blick scheint die Verordnung auf diesen Konflikt keine Antwort zu geben.

Dies führt wiederum zu einer erheblichen Rechtsunsicherheit bei der Erfüllung der Anforderungen an die Sicherheit der Verarbeitung im Zusammenhang mit datenverarbeitenden TOM, wenn mit ihnen gleichzeitig die Vorschriften zur datenschutzrechtlichen Vorabkontrolle tangiert sind. Die damit verbundene Konsequenz können nicht nur in einem Haftungsrisiko für die Verpflichteten liegen, das gerade im unternehmerischen Bereich Schadensersatzansprüche (Art. 82 DS-GVO) und spürbare Bußgelder von bis zu 20 Mio. Euro bzw. 4 % des Jahresumsatzes (Art. 83 DS-GVO) umfassen kann.<sup>27</sup> Zusätzlich tangiert die Frage auch die datenschutzrechtlichen Interessen aller beteiligten, betroffenen Personen und kann zu erheblichen Eingriffen in deren Recht auf Datenschutz führen.<sup>28</sup>

---

<sup>26</sup> Siehe hierzu Art. 83 Abs. 2 S. 2 lit. d) DS-GVO, wonach bei sämtlichen Verstößen gegen die Datenschutz-Grundverordnung die nach Art. 25 und Art. 32 DS-GVO getroffenen technischen und organisatorischen Maßnahmen für die Entscheidung über die Verhängung und Höhe von Geldbußen berücksichtigt werden sollen. Dies wird dahingehend interpretiert, dass eine höhere Sicherheit bußgeldmindernd sein kann, siehe statt vieler zunächst Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 56 f. Siehe hierzu ausführlicher: Kap. 2, B., II., 2. *Gefahren für die – von den TOM – betroffenen Personen*.

<sup>27</sup> Siehe hierzu ausführlicher: Kap. 2, B., I. *Allgemeines Haftungsrisiko*.

<sup>28</sup> Siehe hierzu ausführlicher: Kap. 2, B., II. *Gefahren für den Datenschutz*.

Obwohl die, mit diesem Spannungsverhältnis verbundenen Probleme (in Ansätzen) bereits diskutiert werden,<sup>29</sup> wurde – soweit ersichtlich – bislang noch nicht versucht, das Spannungsverhältnis in seinen Grundlagen zu untersuchen. Die vorliegende Arbeit beschäftigt sich daher mit der Frage, wie die Datenschutz-Grundverordnung auf das Spannungsverhältnis zwischen der datenschutzrechtlichen Vorabkontrolle und der Sicherheit der Verarbeitung im Zusammenhang mit datenverarbeitenden TOM reagiert. Daran anknüpfend soll de lege lata ein Lösungsvorschlag formuliert werden, der Antworten darauf gibt, wie mit technischen und organisatorischen Maßnahmen umzugehen ist, die in diesen Grenzbereich zwischen Art. 32 DS-GVO und Art. 6 DS-GVO fallen.

---

<sup>29</sup> Siehe hierzu ausführlicher: Kap. 2, C., I. *Das Spannungsverhältnis bei datenverarbeitenden TOM in der aktuellen Diskussion.*





## Teil 1

*Datenverarbeitende TOM* im Spannungsverhältnis der Datenschutz-Grundverordnung



## Kapitel 1

# Der Begriff *datenverarbeitende TOM*

### A. Die Bedeutung des Begriffs für die Arbeit

Datenverarbeitende TOM scheinen ein Spannungsverhältnis zwischen der Sicherheit der Verarbeitung nach Art. 32 DS-GVO und der datenschutzrechtlichen Vorabkontrolle i.S.d. Art. 6 DS-GVO zu begründen. Wie sich dieses Spannungsverhältnis im Detail darstellt und welche Probleme hieraus erwachsen können, wird sogleich erörtert.<sup>1</sup> Für die weitere Darstellung ist es jedoch zunächst sinnvoll, den Begriff der „datenverarbeitenden TOM“ zu definieren. Der Begriff wird in der Arbeit häufiger Verwendung finden und soll stellvertretend für das dahinterstehende Spannungsverhältnis stehen.

Bei der nachfolgenden Definition handelt es sich nicht um eine Legaldefinition. Es handelt sich auch nicht um eine Definition, die einer gesonderten, rechtlichen Herleitung bedarf. Vielmehr ist es ein eigener Begriff, der dazu dient, die Probleme in dieser Arbeit verständlicher zu beschreiben. Der Autor stand vor der Herausforderung, einen Begriff zu wählen, dem in der Fachdiskussion einmal ein Wiedererkennungswert zukommt und der unmittelbar mit den betroffenen Themenbereichen assoziiert werden kann. Zum anderen sollten Ähnlichkeiten mit anderen Begriffen weitestgehend ausgeschlossen werden, um Verwechslungsgefahren zu vermeiden. Sollten dennoch Ähnlichkeiten bestehen, ist darauf hinzuweisen, dass hier ein eigenes Begriffsverständnis zugrunde gelegt wird.

### B. Definition

Der Begriff *datenverarbeitende TOM* besteht aus zwei wesentlichen Elementen. „TOM“ oder auch „TOMs“ steht hierbei für die verbreitete Abkürzung von

---

<sup>1</sup> Siehe hierzu: Kap. 2 Datenverarbeitende TOM *im Regelungsbereich zwischen Art. 32 und Art. 6 DS-GVO*.

„technischen und organisatorischen Maßnahmen“.<sup>2</sup> Aufgrund der vielfältigen Verweise auf technische und organisatorische Maßnahmen innerhalb der Verordnung (insb. Art. 24, 25, 32 DS-GVO), wäre eigentlich zu klären, ob die Verordnung hier stets ein einheitliches Verständnis zugrunde legt. Wenigstens in ihrer späteren Wirkung bestehen hier Zweifel, dass für die verschiedenen Vorschriften „dieselben Maßnahmen“ gelten.<sup>3</sup> Es könnte also eine funktionale Auslegung geboten sein, die trotz gleichen Wortlauts unterschiedliche Ergebnisse ermöglicht.<sup>4</sup> Eine Entscheidung in dieser Frage bedarf es für diese Arbeit allerdings nicht, da es sich nach dem zugrundeliegenden Begriffsverständnis nur um technische und organisatorische Maßnahmen i.S.d. Sicherheit der Verarbeitung nach Art. 32 Abs. 1 DS-GVO handelt. Man könnte auch von „Sicherheitsmaßnahmen“ sprechen.<sup>5</sup> (Datenverarbeitende) TOM sind somit erstmal nur eine (Unter-)Gruppe aller technischen und organisatorischen Maßnahmen, die der Sicherheit nach Art. 32 Abs. 1 DS-GVO dienen. Dieser Begriffsteil bezweckt damit vorrangig, den sperrigen Begriff der „technischen und organisatorischen Maßnahmen“ abzukürzen und die Verbindung zu Art. 32 Abs. 1 DS-GVO herzustellen.

Das zweite Element wird durch den Begriffsteil „*datenverarbeitend*“ beschrieben. Hiermit soll ausgedrückt werden, dass bei dem Einsatz der Sicherheitsmaßnahmen Daten verarbeitet werden. Anders als der Wortlaut dies zunächst erscheinen lässt, handelt es sich jedoch nicht um die Verarbeitung irgendwelcher Daten. Unter „*datenverarbeitend*“ ist hier konkret die Verarbeitung personenbezogener Daten, i.S.d. Legaldefinition des Art. 4 Nr. 1 DS-GVO, zu

---

<sup>2</sup> DatKomm/*Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 3; *Taeger/Gabel/Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 12; *Plath/Grages*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 4; *Auer-Reinsdorff/Conrad/Conrad/Treeger*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 113; *Seufert*, ZD 2023, S. 256, 257; *Johannes/Geminn*, InTeR 2021, S. 140, 141; *John/Schaller*, CR 2022, S. 156, 156.

<sup>3</sup> Siehe hierzu in Ansätzen: Kap. 2, C., I. *Das Spannungsverhältnis bei datenverarbeitenden TOM in der aktuellen Diskussion*.

<sup>4</sup> Siehe zur funktionalen Auslegung im Europäischen Recht statt vieler EuGH, verb. Rs. C-403/08, C-429/08 (Football Association Premier League u.a.), ECLI:EU:C:2011:631 = ZUM 2011, 803, Rn. 187 f.; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81. Siehe hierzu ausführlicher Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen* und dort die Nachweise in Fn. 142.

<sup>5</sup> *Schneider*, Datenschutz, 2. Aufl. 2019, S. 259.

verstehen. Dass der Wortlaut weitergefasst ist als die Verarbeitung personenbezogener Daten, ist eine sprachliche Ungenauigkeit, die hier in Kauf genommen werden muss. Andernfalls dürfte der Begriff ebenfalls zu einer sperrigen Formulierung verkommen und der Verständlichkeit schaden, die die Definition eigentlich gewährleisten soll.

Weiterhin ist für den Begriff in dieser Arbeit von der Prämisse auszugehen, dass die zugrundeliegende Datenverarbeitung essenziell für die Funktionsweise der Maßnahme ist. Ohne die Verarbeitung personenbezogener Daten gelten die Maßnahme als wirkungslos bei der Gewährleistung der Sicherheit der Verarbeitung.

Zusammengenommen sind datenverarbeitende TOM also technische und organisatorische Maßnahmen i.S.d. Art. 32 Abs. 1 DS-GVO, die ihrerseits personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO verarbeiten.



## Kapitel 2

### *Datenverarbeitende TOM im Regelungsbereich zwischen Art. 32 und Art. 6 DS-GVO*

#### A. Begründung eines Spannungsverhältnisses zwischen Art. 32 und Art. 6 DS-GVO

##### *I. Die Implementierung von (datenverarbeitenden) TOM nach Art. 32 DS-GVO*

Ausgangspunkt für ein mögliches Spannungsverhältnis bei datenverarbeitenden TOM stellt die Sicherheit der Verarbeitung nach Art. 32 DS-GVO dar. Gem. Art. 32 Abs. 1 DS-GVO haben Verantwortliche und Auftragsverarbeiter (der Einfachheit halber hier auch als „Datenverarbeiter“ zusammengefasst)<sup>1</sup> technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Was die Datenschutz-Grundverordnung hierbei unter einem, dem Risiko angemessenen Schutzniveau verstehen möchte und welche Ziele sie hiermit verfolgt, erschließt sich bei einer ersten Betrachtung des Normtextes nicht unmittelbar. Aufgrund einer komplizierten Normstruktur und der damit verbundenen Gefahr von Missverständnissen verdient dieser Punkt an späterer Stelle eine genauere Betrachtung.<sup>2</sup>

Um das Problem datenverarbeitender TOM jedoch in den Grundlagen nachvollziehen zu können, reicht zunächst die Erkenntnis, dass nach Art. 32 DS-GVO technische und organisatorische Maßnahmen getroffen werden müssen, um ein bestimmtes Schutzniveau zu gewährleisten und damit den Anforderungen nach Art. 32 DS-GVO nachzukommen. Es besteht folglich eine zu konkretisierende Pflicht zur Implementierung technischer und organisatorischer Maßnahmen.

---

<sup>1</sup> Siehe ebenfalls zur Zusammenfassung dieser beiden unter den Begriff „Datenverarbeiter“: *Gierschmann*, ZD 2016, S. 51, 51.

<sup>2</sup> Siehe hierzu ausführlicher: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO*.

Datenverarbeitende TOM als eine Untergruppe dieser Maßnahmen können daher grundsätzlich hiervon umfasst sein und es könnte somit eine Pflicht bestehen, datenverarbeitende TOM zu implementieren, um das Schutzniveau zu gewährleisten. Damit könnten datenverarbeitende TOM unter die Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO fallen.

## II. Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO

Datenverarbeitende TOM verarbeiten ihrerseits personenbezogene Daten. Das europäische Datenschutzrecht verfolgt den Ansatz, dass jede Verarbeitung personenbezogener Daten eine Beeinträchtigung der Rechte, der von ihr betroffenen Personen darstellt.<sup>3</sup> Eine Verarbeitung ist daher nicht frei möglich.<sup>4</sup> Zum Schutz der betroffenen Person ist im Vorfeld stets zu prüfen, ob eine Datenverarbeitung rechtmäßig vorgenommen werden darf. Für die Rechtmäßigkeit der Datenverarbeitung bedarf es hierzu einer Rechtsgrundlage, die zentral<sup>5</sup> in Art. 6

---

<sup>3</sup> Vgl. Kuner/Bygrave/Docksey/Kotschy, GDPR, 2020, p. 329; Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 3, Rn. 51, siehe dort auch *Nebel*, § 3, Rn. 94. Siehe auch Simitis/Hornung/Spiecker gen. Döhmman/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 1 DS-GVO, Rn. 4, wonach das Datenschutzrecht „präventiv“ ausgerichtet ist; siehe zu dieser präventiven Ausrichtung auch Auernhammer/v. Lewinski, 8. Aufl. 2024, Einführung, Rn. 18 f., der von einer „Vorfeldschutz-Kaskade“ spricht und diese präventive Ausrichtung auch kritisch betrachtet; ebenfalls kritisch zu dieser präventiven Ausrichtung *Veil*, NVwZ 2018, S. 686, 688 f.

<sup>4</sup> Den Grundsatz des Verbots jeder Datenverarbeitung heben u.a. heraus: Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 334; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 10; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 2; Klein, Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?, in: FS Taeger, 2020, S. 235, 236; siehe auch Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 1a, allerdings mit dem Verweis, dass die Erlaubnis der Verarbeitung keine Ausnahme darstellt. Kritisch zum „Verbotsprinzip“ Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 3, Rn. 50; Roßnagel, NJW 2019, S. 1, 4 f., wobei die Kritik weniger in der Frage der Rechtsfolge liegen dürfte, sondern wohl mit den Implikationen, die mit einem solchen „Verbot“ einhergehen.

<sup>5</sup> Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 1; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 20; Roßnagel/Nebel, Das neue Datenschutzrecht, 2018, § 3, Rn. 95; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 4; Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 370; vgl. Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 1, be-



Abs. 1 DS-GVO aufgeführt werden.<sup>6</sup> Dieses Prinzip wird in der deutschsprachigen Literatur verbreitet als „Verbot mit Erlaubnisvorbehalt“<sup>7</sup> klassifiziert<sup>8</sup> und bei den Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO spricht man auch von „Erlaubnistatbeständen“<sup>9</sup>.

Die Klassifizierung als „Verbot mit Erlaubnisvorbehalt“ ist allerdings in Bezug auf die Datenschutz-Grundverordnung umstritten.<sup>10</sup> Eine Entscheidung

---

zeichnet sie als die „wichtigsten Erlaubnistatbestände“. Für besondere Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DS-GVO listet dessen Absatz 2 ähnliche Tatbestände auf und wirft die Frage des Verhältnisses beider Vorschriften zueinander auf. Siehe hierzu Kap. 3, C., V. *Beschränkung auf die Rechtmäßigkeit der Verarbeitung nach Art. 6 DS-GVO* und insb. die Nachweise in Fn. 18.

<sup>6</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 10; Simitis/Hornung/Spiecker gen. Döhmman/*Albrecht*, Datenschutzrecht, 2019, Einf. Art. 6 DS-GVO, Rn. 1; Kühling/*Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 13; Kuner/*Bygrave/Docksey/Kotschy*, GDPR, 2020, p. 325.

<sup>7</sup> Siehe allgemein zum „Verbot mit Erlaubnisvorbehalt“: *Schmid*, DÖV 1954, S. 243 f.; *Maurer/Waldhoff*, Allgemeines Verwaltungsrecht, 21. Aufl. 2024, § 9, Rn. 52 ff.; *Ipsen*, Allgemeines Verwaltungsrecht, 11. Aufl. 2019, Rn. 387 f.; *Detterbeck*, Allgemeines Verwaltungsrecht, 21. Aufl. 2023, Rn. 504; siehe auch weitergehend *Cherng*, Verbote mit Erlaubnisvorbehalt im Rechte der Ordnungsverwaltung, 2001.

<sup>8</sup> Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 5; Kühling/*Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 1, 11; Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 1a; Ehmann/*Selmayr/Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 1; Plath/*Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 2; Spindler/*Schuster/Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 1; *Klein*, Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?, in: FS Taeger, 2020, S. 235, 236; *Ziegenborn/v. Heckel*, NVwZ 2016, S. 1585, 1586; *Knyrim/Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.49; *Moos/Schefzig/Arning/Moos*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 4, Rn. 4.

<sup>9</sup> Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 1a; Taeger/*Gabel/Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 20 ff.; Kühling/*Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 1a, siehe auch die Überschrift vor Rn. 11; *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 12, Rn. 1; *Ziegenborn/v. Heckel*, NVwZ 2016, S. 1585, 1586 f.

<sup>10</sup> Weiterführend zur Kritik, aber in unterschiedlicher Ausformung und Reichweite: *Gola/Heckmann/Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 2, „*Verbotsprinzip*“; *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 334, sprechen vom „*Verbot mit Zulässigkeitstatbeständen*“. Grundlegender in der Kritik: BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO

über die „richtige“ Bezeichnung dieses Prinzips ist für das Ergebnis dieser Arbeit unerheblich und bedarf daher keiner weiteren Diskussion. Denn von der Diskussion unberührt und für die weitere Untersuchung allein entscheidend, bleibt das Erfordernis einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Die vor der Verarbeitung personenbezogener Daten erforderliche Prüfung einer bestehenden Rechtsgrundlage stellt damit die Mindestvoraussetzung für jede Verarbeitung personenbezogener Daten dar. Nachfolgend wird daher von der „datenschutzrechtlichen Vorabkontrolle“ und dem Begriff der „Rechtsgrundlage“<sup>11</sup> gesprochen.

Das Datenschutzrecht stellt insofern im Rahmen der Vorabkontrolle Anforderungen an jede Datenverarbeitung. Aufgrund der ihnen zugrundeliegenden Datenverarbeitung unterfallen damit auch datenverarbeitende TOM (indirekt) dieser Kontrolle. Kann die ihnen zugrundeliegende Verarbeitung auf keine Rechtsgrundlage gestützt werden, dürfen die Daten nicht verarbeitet werden. Die Verarbeitung personenbezogener Daten ist jedoch essenziell für die Funktionsweise der Maßnahmen.<sup>12</sup> Eine Entscheidung über die Rechtmäßigkeit der Datenverarbeitung könnte damit faktisch auch auf die Implementierung der technischen und organisatorischen Maßnahmen selbst durchschlagen.

---

(Stand: August 2023), Rn. 11; Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 3, Rn. 50; Roßnagel, NJW 2019, S. 1, 4 f., „Erlaubnisprinzip“; Simitis/Hornung/Spiecker gen. Döhmann/Albrecht, Datenschutzrecht, 2019, Einf. Art. 6 DS-GVO, Rn. 1, spricht von einem „datenschutzrechtlichen Erlaubnisvorbehalt“ (siehe auch dort die Fn. 1); auch Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 2, Rn. 2; Specht/Mantz/Mantz/Marosi, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 50, „Begriff des Verarbeitungsrechtfertigungszwangs“; siehe auch kritisch zu dem Begriff Wybitul/Pöiters/Rauer, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 7.

<sup>11</sup> Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 3, Rn. 36; Specht/Mantz/Mantz/Marosi, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 50; siehe auch Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 1 ff. unter der Verwendung der Begriffe „Rechtsgrund“ oder „Rechtsgrundlage“. Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 334, 370 verwenden den Begriff „Zulässigkeitstatbestände“; so stellenweise auch Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 18; Knyrim/Haidinger, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.49, 5.59, bevorzugen jedoch den Begriff „Rechtmäßigkeitsgrundlage“.

<sup>12</sup> Siehe zu dieser Prämisse: Kap. 1, B. Definition.

*III. Konflikt zwischen Art. 32 DS-GVO und Art. 6 DS-GVO*

Datenverarbeitende TOM befinden sich somit in einer Schnittmenge zwischen der Sicherheit der Verarbeitung nach Art. 32 DS-GVO und der datenschutzrechtlichen Vorabkontrolle nach Art. 6 DS-GVO. Die erste Betrachtung zeigt, dass nach Art. 32 Abs. 1 DS-GVO eine Pflicht besteht, technische und organisatorische Maßnahmen zu implementieren, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Implementierung datenverarbeitender TOM als Erfüllung dieser Pflicht könnte sich allerdings zu einem Problem erweisen. Denn ob diese Maßnahmen rechtskonform implementiert werden können, setzt die Rechtmäßigkeit der ihnen zugrundeliegenden Datenverarbeitung voraus. Solange die Verarbeitung personenbezogener Daten nicht auf einer Rechtsgrundlage i.S.d. Art. 6 DS-GVO gestützt werden kann, darf die Verarbeitung nicht vorgenommen und faktisch auch die Maßnahme nicht implementiert werden.

Für die Sicherheit der Verarbeitung können diese ergänzenden Anforderungen aus der datenschutzrechtlichen Vorabkontrolle zum Problem werden, wenn die Prüfung nach Art. 6 DS-GVO ergibt, dass die Verarbeitung datenschutzrechtswidrig ist und sowohl sie als auch die Maßnahmen nicht vorgenommen werden dürfen. Damit könnte Art. 6 DS-GVO über die Erfüllung der Pflichten nach Art. 32 DS-GVO (mit-)entscheiden. Im Extremfall könnte dies zu einem Konflikt zwischen den beiden Vorschriften führen, bei dem Art. 32 DS-GVO mit der Implementierung von technischen und organisatorischen Maßnahmen zu einer Handlung verpflichtet, die durch die datenschutzrechtliche Vorabkontrolle verboten wäre.<sup>13</sup> Es käme zu einem Widerspruch innerhalb der Verordnung.

## B. Risiken aus dem Spannungsverhältnis

Aus diesem Spannungsverhältnis können sich mehrere Risiken sowohl für die Datenverarbeiter als auch für betroffene Personen ergeben.

---

<sup>13</sup> Dieses Problem sieht auch Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 58; ähnlich auch Hoeren/Sieber/Holzner/Schmitz, Hdb. Multimedia-Recht, Stand: 59. EL, 2023, Teil 16.2, Rn. 361 f. (Stand: Oktober 2020).

### I. Allgemeines Haftungsrisiko

Allgemein sorgt das Spannungsverhältnis für Unsicherheiten bei der rechtskonformen Umsetzung der Sicherheit der Verarbeitung, die in einem Verstoß gegen Art. 32 DS-GVO resultieren kann, wenn dadurch keine oder unzureichende Maßnahmen getroffen werden.<sup>14</sup> Ein Verstoß kann zu Sanktionen nach der Datenschutz-Grundverordnung führen. Besonders einschneidend sind hier mögliche Schadensersatzansprüche betroffener Personen nach Art. 82 DS-GVO und – gerade im privatrechtlichen Bereich –<sup>15</sup> die Verhängung von Bußgeldern durch die Aufsichtsbehörden i.S.d. Art. 83 DS-GVO.

So drohen bei einem Verstoß gegen Art. 32 DS-GVO Bußgelder i.H.v. bis zu 2 % des Jahresumsatzes<sup>16</sup> oder<sup>17</sup> 10 Mio. Euro (Art. 83 Abs. 4 lit. a) DS-GVO).<sup>18</sup>

<sup>14</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 40a; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 30; vgl. *Ihwas*, NZWiSt 2021, S. 289, 290 f., wonach bereits nicht hinreichende Maßnahmen ein Bußgeld nach sich ziehen können.

<sup>15</sup> Gegenüber Behörden und (anderen) öffentlichen Stellen kann der Mitgliedstaat entscheiden, ob ein Bußgeld nach Art. 83 DS-GVO verhängt werden kann, vgl. Art. 83 Abs. 7 DS-GVO. In Deutschland kann gegenüber Behörden und öffentliche Stellen kein Bußgeld verhängt werden, vgl. § 43 Abs. 3 BDSG. Siehe hierzu auch Simitis/Hornung/Spiecker gen. Döhmann/*Boehm*, Datenschutzrecht, 2019, Art. 83 DS-GVO, Rn. 55; Taeger/Gabel/*Moos/Schefzig*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 83 DS-GVO, Rn. 156.

<sup>16</sup> Sofern es sich um ein Unternehmen handelt.

<sup>17</sup> Welche Größe für die Bußgeldberechnung angesetzt wird, entscheidet sich danach, welcher Betrag höher ist, vgl. Art. 83 Abs. 4, 5 DS-GVO.

<sup>18</sup> Art. 32 DS-GVO steht im Zusammenhang des Datenschutzgrundsatzes nach Art. 5 Abs. 1 lit. f) DS-GVO, statt vieler Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 1; siehe hierzu: Kap. 4, A. *Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.* Daher wird teilweise darauf hingewiesen, dass ein Verstoß gegen Art. 32 DS-GVO gleichzeitig einen Verstoß gegen Art. 5 DS-GVO darstellen kann. Allgemein zu dieser Möglichkeit: *Brams*, ZD 2023, S. 484, 486; *Bartels/Backer*, DuD 2018, S. 214, 219; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 13, wohl nur bei gravierender Missachtung der Anforderungen an die Sicherheit; ähnlich *Keppeler/Berning*, DStR 2018, S. 91, 92, die jedenfalls bei ihrem Beispiel auf einen gravierenden Verstoß abstellen; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 17, die aber dann wohl eher auf die speziellere Norm abstellen will; Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 88, die einen Verstoß des Art. 5 Abs. 1 lit. f) DS-GVO nur annehmen möchten, wenn keine Maßnahmen getroffen wurden; vgl. auch *Poncza*, ZD 2023, S. 8, 12, der auf die Möglichkeit einer Anknüpfung sowohl an den höheren als auch

Das Haftungsrisiko aus dem Spannungsverhältnis betrifft jedoch nicht nur die Gefahr eines Verstoßes gegen Art. 32 DS-GVO. Denkbar ist auch ein Verstoß gegen Art. 6 DS-GVO, wenn Datenverarbeiter datenverarbeitende TOM zur Erfüllung ihrer Pflichten nach Art. 32 DS-GVO implementieren, die i.S.d. Art. 6 DS-GVO rechtswidrig sind. Ein Verstoß gegen Art. 6 DS-GVO kann dabei sogar Bußgelder i.H.v. 4 % des Jahresumsatzes oder 20 Mio. Euro gem. Art. 83 Abs. 5 lit. a) DS-GVO nach sich ziehen.

Bei dem Versuch das Spannungsverhältnis selbst zu lösen, stehen Datenverarbeiter vor der Herausforderung, die Anforderungen sowohl nach Art. 32 DS-GVO als auch Art. 6 DS-GVO zu erfüllen, um nicht die dahinterstehenden Sanktionen auszulösen. Die Lösung in dieser Frage kann daher nicht sein, Datenverarbeiter hier „allein zu lassen“ und vor die „Wahl zu stellen“, ob sie lieber das höhere (4 % bzw. 20 Mio. Euro) oder das niedrigere (2 % bzw. 10 Mio. Euro) Haftungsrisiko tragen „möchten“.<sup>19</sup>

## *II. Gefahren für den Datenschutz*

Das Spannungsverhältnis und die damit bestehenden Unsicherheiten beim Umgang mit datenverarbeitenden TOM könnte zusätzlich zu Gefahren für den Datenschutz selbst führen.

### *1. Gefahren für die – nach Art. 32 DS-GVO zu schützenden – betroffenen Personen*

Diese Gefahren betreffen einmal die Sicherheit der Verarbeitung und die datenschutzrechtlichen Interessen der betroffenen Personen, deren personenbezogene Daten nach Art. 32 DS-GVO geschützt werden sollen. Denn die Unsicherheiten der Datenverarbeiter hinsichtlich der Erfüllung des Art. 32 DS-GVO schlagen sich direkt auf die Datenschutzinteressen der betroffenen Personen

---

an den niedrigeren Bußgeldtatbestand hinweist, dies im Ergebnis aber für (verfassungs-) und europarechtlich bedenklich hält. Ein Verstoß gegen Art. 5 DS-GVO unterliegt dem höheren Bußgeldrahmen (4 % Jahresumsatz bzw. 20 Mio. Euro), vgl. Art. 83 Abs. 5 lit. a) DS-GVO. Auf das Verhältnis zwischen Datenschutzgrundsätze und spezieller Vorschriften kann hier nicht näher eingegangen werden. Siehe ausführlicher zum Problem der Geldbußen wegen Verstößen nach Art. 5 DS-GVO (auch im Zusammenhang des Verhältnisses zu spezielleren Vorschriften) Klaas/Momsen/Wybitul/*Wybitul*, *Datenschutzsanktionenrecht*, 2023, § 3, Rn. 44 ff.

<sup>19</sup> Vgl. zu diesem Problem auch Hornung/Schallbruch/*Jandt*, *IT-Sicherheitsrecht*, 2021, § 17, Rn. 58.

durch. Unterlassen Datenverarbeiter die Implementierung datenverarbeitender TOM aufgrund deren Eingriffe in den Datenschutz, könnte dies dazu führen, dass die Anforderungen an die Sicherheit der Verarbeitung nicht erreicht werden, die verarbeiteten Daten somit nicht ausreichend geschützt werden und dies letztlich den Datenschutzinteressen der betroffenen Personen schaden kann.

Eine solche „Verletzung“ der Datenschutzinteressen muss aber nicht einzig auf die Unsicherheiten der Datenverarbeiter bei der Umsetzung der rechtlichen Anforderungen zurückzuführen sein. Die Unsicherheit über die rechtlichen Rahmenbedingungen besteht allgemein und könnte von Datenverarbeitern auch gezielt und unter Inkaufnahme eines Haftungsrisikos ausgenutzt werden, um sich Aufwendungen zur Gewährleistung der Sicherheit zu ersparen. Datenverarbeiter könnten in diesem Fall die Eingriffe in den Datenschutz durch datenverarbeitende TOM als Grund in einem rechtlichen Graubereich vorschieben, um ein niedrigeres Maß an Sicherheit zu gewährleisten.

## 2. Gefahren für die – von den TOM – betroffenen Personen

Die Gefahren für den Datenschutz bestehen zudem nicht nur bei betroffenen Personen, deren Daten nach Art. 32 DS-GVO zu schützen sind. Das Spannungsverhältnis gefährdet auch den Datenschutz der Personen, deren personenbezogene Daten durch die datenverarbeitenden TOM verarbeitet werden sollen. Um den Anforderungen an die Sicherheit der Verarbeitung nachzukommen, könnten Datenverarbeiter datenverarbeitende TOM einsetzen, deren Verarbeitung personenbezogener Daten nach dem Datenschutzrecht nicht zu rechtfertigen ist und hierbei die geschützten Interessen der betroffenen Personen verletzen.

Erschwerend könnte noch hinzukommen, dass die Datenschutz-Grundverordnung scheinbar auch gezielt Anreize schaffen möchte, ein „Mehr“ an Sicherheit nach Art. 32 DS-GVO zu gewährleisten. So soll bei *jedem* Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung im Rahmen der Bußgeldbemessung der Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters berücksichtigt werden, vgl. Art. 83 Abs. 2 S. 2 lit. d) DS-GVO. Ausweislich des Art. 83 Abs. 2 S. 2 lit. d) DS-GVO kommt es dabei auch auf die von ihnen getroffenen technischen und organisatorischen Maßnahmen nach Art. 25 und Art. 32 DS-GVO an. Dies wird teilweise dahingehend interpretiert, dass eine „überschießende“ Implementierung technischer und organisatorischer

Maßnahmen – im Falle des Art. 32 DS-GVO also ein „Mehr“ an Sicherheit – bei jedem Verstoß auch bußgeldmindernd berücksichtigt werden kann.<sup>20</sup>

Aus Sicht des Datenschutzes ist eine solche Berücksichtigung nachvollziehbar, da u.a. höhere Sicherheitsanforderungen – jedenfalls im begrenzten Umfang – die Risiken eines Datenschutzverstoßes abmildern können.<sup>21</sup> Aus Sicht der Datenverarbeiter könnte hiermit ein Anreiz geschaffen werden, u.a. eine hohe Sicherheit nach Art. 32 DS-GVO für jede Verarbeitung zu gewährleisten.<sup>22</sup> In Bezug auf das hier geschilderte Spannungsverhältnis könnte dies allerdings dazu führen, dass Datenverarbeiter sich auch vermehrt datenverarbeitender TOM bedienen könnten, um diese höhere Sicherheit zu erreichen. Die Berücksichtigung der Risiken eines damit in Verbindung stehenden Eingriffs in die datenschutzrechtlichen Interessen der, von den Maßnahmen betroffenen Personen könnte dabei allerdings „auf der Strecke bleiben“.

Ähnlich wie im Zusammenhang mit der Sicherheit der Verarbeitung kann eine solche Verletzung der datenschutzrechtlichen Interessen der, von den datenverarbeitenden TOM betroffenen Personen aber auch von den Datenverarbeitern beabsichtigt sein. So könnten Datenverarbeiter versuchen, unter dem

---

<sup>20</sup> Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 57; Spindler/Schuster/*Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 29; Ehmann/Selmayr/*Nemitz*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83 DS-GVO, Rn. 20; Sydow/Marsch/*Popp*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 83 DS-GVO, Rn. 16; Taeger/Gabel/*Moos/Schefzig*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 83 DS-GVO, Rn. 84; siehe allgemein als Anreiz Schuster/Grütz-macher/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 13, allerdings (wohl versehentlich) mit Verweis auf lit. e); Specht/Mantz/*Schneider*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 15, Rn. 104; vgl. EDSA, Leitlinien 04/2022, Rn. 81, wobei eine abmildernde Berücksichtigung wohl die Ausnahme darstellen soll; auch für eine abmildernde Berücksichtigung nur im Ausnahmefall Kühling/Buchner/*Bergt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 83 DS-GVO, Rn. 55; wohl gegen eine abmildernde Berücksichtigung Jandt/Steidle/*Richter*, Datenschutz im Internet, 2018, B. IV., Rn. 72, der nur auf die Möglichkeit der Erhöhung verweist.

<sup>21</sup> Vgl. Taeger/Gabel/*Moos/Schefzig*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 83 DS-GVO, Rn. 84; siehe auch Kühling/Buchner/*Bergt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 83 DS-GVO, Rn. 55, in umgekehrter Situation, dass unzureichende Maßnahmen das Risiko erhöhen können.

<sup>22</sup> Vgl. Ehmann/Selmayr/*Nemitz*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83 DS-GVO, Rn. 20.

Vorwand zur Gewährleistung der Sicherheit der Verarbeitung, personenbezogene Daten durch datenverarbeitende TOM zu verarbeiten, die sie andernfalls nicht hätten verarbeiten dürfen.<sup>23</sup> Einmal „im Besitz“ dieser Daten könnten sie diese dann zu anderen Zwecken weiterverarbeiten.<sup>24</sup> Auch hier könnte man versuchen, die bestehenden Unsicherheiten im Rahmen datenverarbeitender TOM auszunutzen, um eigene Ziele zu verfolgen.

### III. Zwischenergebnis

Ohne eine Lösung führen die Unsicherheiten aus dem Spannungsverhältnis zu einem rechtlichen Graubereich, der sich auf Datenverarbeiter und betroffene Personen gleichermaßen auswirken kann. Um sowohl die Haftungsrisiken auf der Seite der Datenverarbeiter als auch die Gefahren für den Datenschutz der betroffenen Personen einzudämmen, bedarf es einer solchen Lösung des Spannungsverhältnisses.

## C. Die Bedeutung datenverarbeitender TOM

### I. Das Spannungsverhältnis bei datenverarbeitenden TOM in der aktuellen Diskussion

Das Spannungsverhältnis bei datenverarbeitenden TOM und dessen rechtliche Auswirkungen konnten zwar abstrakt beschrieben werden.<sup>25</sup> Ein wirkliches Verständnis über das Ausmaß dieses Problems wird allerdings erst deutlich, wenn man sich einmal relevante Maßnahmen aus der Praxis betrachtet. Zunächst ist darauf hinzuweisen, dass datenverarbeitende TOM wohl keine reinen Ausnahmeerscheinungen darstellen und vor allem mit der fortschreitenden Digitalisierung weiter an Bedeutung gewinnen werden. Die Gründe hierfür liegen

---

<sup>23</sup> Auf diese Missbrauchsgefahr weisen auch *Schulte/Wambach*, DuD 2020, S. 462, 465 f. hin.

<sup>24</sup> Das Datenschutzrecht stellt zwar spezielle Anforderungen daran, unter welchen Bedingungen Daten für andere Zwecke verarbeitet werden dürfen (vgl. hierzu insb. Art. 5 Abs. 1 lit. b), Art. 6 Abs. 4 DS-GVO). Sind die Daten jedoch einmal erhoben, kann es in vielen Fällen schwer sein, von außen festzustellen, ob Daten für andere Zwecke verarbeitet werden.

<sup>25</sup> Siehe hierzu: Kap. 2, A. *Begründung eines Spannungsverhältnisses zwischen Art. 32 und Art. 6 DS-GVO* und B. *Risiken aus dem Spannungsverhältnis*.



einmal in der Ubiquität von Datenverarbeitungen durch die Digitalisierung und damit die schrumpfenden „datenfreien“ Bereiche.<sup>26</sup> Dies wird dann zwangsweise auch die Funktionsweise von technischen und organisatorischen Maßnahmen für die Sicherheit der Verarbeitung treffen. Dazu kommt die Auslegung des Begriffs der personenbezogenen Daten i.S.d. Datenschutzrechts.

Nach der Legaldefinition handelt es sich bei „*personenbezogenen Daten*“<sup>27</sup> um „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen [...]*“ (vgl. Art. 4 Nr. 1 DS-GVO)<sup>28</sup>. Der Begriff der personenbezogenen Daten wird in jedem Fall weit verstanden.<sup>29</sup> Bei der zunehmenden Zahl von (jeglichen) Datenverarbeitungen, gelangen diese durch den weiten Begriff der personenbezogenen Daten daher schnell in den Anwendungsbereich des Datenschutzrechts und unterliegen dann dem datenschutzrechtlichen Kontrollsystem.

Bereits jetzt dürften eine Vielzahl von Maßnahmen für die Sicherheit nach Art. 32 DS-GVO personenbezogene Daten verarbeiten.<sup>30</sup> Daher verwundert es

---

<sup>26</sup> Siehe hierzu *Rofsnagel/Müller*, CR 2004, S. 625 ff.; *Kübling*, Die Verwaltung 2007, S. 155 ff.; vgl. auch *Kübling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 2 ff.; *Ehmann/Selmayr/Selmayr/Ehmann*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung DS-GVO, Rn. 19; *Specht/Mantz/Krätschmer*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 6, Rn. 33, ebenfalls mit dem ergänzenden Verweis auf den weiten Begriff „personenbezogener Daten“ (siehe hierzu sogleich).

<sup>27</sup> Englisch: „*personal data*“, Französisch: „*données à caractère personnel*“, Spanisch: „*datos personales*“, Italienisch: „*dato personale*“, Niederländisch: „*persoonsgegevens*“.

<sup>28</sup> Englisch: „*any information relating to an identified or identifiable natural person [...]*“, Französisch: „*toute information se rapportant à une personne physique identifiée ou identifiable [...]*“, Spanisch: „*toda información sobre una persona física identificada o identificable [...]*“, Italienisch: „*qualsiasi informazione riguardante una persona fisica identificata o identificabile [...]*“, Niederländisch: „*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon [...]*“.

<sup>29</sup> EuGH, Rs. C-180/21 (Inspektor v Inspektorata kam Visshia sadeben savet [Finalités du traitement de données - Enquête pénale]), ECLI:EU:C:2022:967 = BeckRS 2022, 34896, Rn. 70; EuGH, Rs. C-434/16 (Nowak), ECLI:EU:C:2017:994 = NJW 2018, S. 767, Rn. 34, noch zur Datenschutzrichtlinie; *Paal/Pauly/Ernst*, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 DS-GVO, Rn. 3; *Simitis/Hornung/Spiecker gen. Döhmann/Karg*, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO, Rn. 3; *Speicker gen. Döhmann u.a./Farinbo*, GDPR, 2023, Art. 4(1) GDPR, Rn. 3; *Kühling/Buchner/Klar/Kübling*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 1 DS-GVO, Rn. 8.

<sup>30</sup> Siehe hierzu auch die nachfolgenden Beispiele unter: Kap. 2, C., II. „*Überwachungsmaßnahmen*“ als Anwendungsfeld datenverarbeitender TOM.

etwas, dass in der datenschutzrechtlichen Diskussion das Spannungsverhältnis hinter den datenverarbeitenden TOM scheinbar nur oberflächlich diskutiert wird. Soweit ersichtlich wurde bislang noch nicht versucht, das Spannungsverhältnis zwischen diesen beiden Bereichen des Datenschutzrechts in seinen Grundlagen zu untersuchen und einen Lösungsvorschlag anzubieten.

Zwar werden die Anforderungen der datenschutzrechtlichen Vorabkontrolle i.S.d. Art. 6 DS-GVO bei Maßnahmen, die man als datenverarbeitende TOM einstufen könnte, untersucht.<sup>31</sup> Welche Folgen datenverarbeitende

---

<sup>31</sup> *Piltz*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351 ff., allgemein zur Frage, ob Art. 32 DS-GVO i.V.m. Art. 6 Abs. 3 DS-GVO als Rechtsgrundlage dient; *Schuster/Grützmaker/Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 7, zum Problem von Datenverarbeitungen im Rahmen des Art. 32 DS-GVO und der Frage, ob Art. 32 DS-GVO als Rechtsgrundlage für die Verarbeitung dient; auch *Freund u.a./Schmidt*, DSGVO, 2023, Art. 6 DS-GVO, Rn. 49 f.; *Hoeren/Sieber/Holznapel/Schmitz*, Hdb. Multimedia-Recht, Stand: 59. EL. 2023, Teil 16.2, Rn. 359 ff. (Stand: Oktober 2020), zu Datenverarbeitungen im Zusammenhang mit Art. 32 DS-GVO; *Hornung/Schallbruch/Jandt*, IT-Sicherheitsrecht, 2021, § 17, Rn. 54 ff., allgemein zur „[d]atenschutzrechtlichen Zulässigkeit von Maßnahmen der IT-Sicherheit“; ähnlich *Kipker/Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 40 ff.; auch *Taeger/Pohle/Deusch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 328 f. (Stand: Mai 2022); *Sassenberg/Faber/Mantz/Spittka*, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 176; v. *Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 41 ff. Siehe auch zu einzelnen Maßnahmen, die als solche i.S.d. Art. 32 DS-GVO verstanden werden könnten: *Joos/Nägele*, DuD 2022, S. 578 ff., hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten für Softwaretestungen (auch im Zusammenhang des Art. 32 DS-GVO); *Poncza*, ZD 2023, S. 8 ff., anhand von „Penetration Tests“; *Schlegel*, ZD 2020, S. 243 ff., zu „Data-Loss-Prevention(DLP)-Software“; ebenfalls hierzu *Auer-Reinsdorff/Conrad/Conrad/Treger*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 296; *Krügel*, MMR 2017, S. 795 ff. unter anderem anhand der datenschutzrechtlichen Zulässigkeit von Angriffserkennungssystemen im Zusammenhang mit Art. 32 DS-GVO; *Schulte/Wambach*, DuD 2020, S. 462 ff., unter anderem anhand von Log files zur „Aufklärung von IT-Sicherheitsvorfällen“ (S. 464 f.). Siehe auch *Byers/Winkler/Stelter*, NZA 2023, S. 457 ff. zur datenschutzrechtlichen Zulässigkeit von biometrischen Kontrollen, vorrangig anhand von Art. 9 DS-GVO. Siehe auch einige der Nachweise im Rahmen der nachfolgenden Beispiele: Kap. 2, C., II. „Überwachungsmaßnahmen“ als Anwendungsfeld datenverarbeitender TOM.

TOM und das Spannungsverhältnis hingegen auf den Pflichtenumfang der Sicherheit der Verarbeitung haben, wurden – soweit ersichtlich – noch nicht ausführlich behandelt.<sup>32</sup>

Allerdings ist dabei jedoch anzuerkennen, dass viele Maßnahmen nicht zwangsweise auch TOM i.S.d. Art. 32 DS-GVO darstellen müssen. Dass, was sie zu TOM i.S.d. Art. 32 DS-GVO qualifiziert, ergibt sich nicht zwingend aus ihrer Funktionsweise, sondern eher den Zielen ihres Einsatzes.<sup>33</sup> Im Falle des Art. 32 DS-GVO also die Gewährleistung der Sicherheit der Verarbeitung. Sowohl die Maßnahmen als auch die Datenverarbeitung können meist auch für andere Ziele eingesetzt werden. Als sehr plastisches Beispiel könnte man hier den Einsatz von Überwachungskameras nennen. Werden Überwachungskameras eingesetzt, um die Zutritte zu einem Serverraum mit sensiblen, personenbezogenen Daten zu überwachen und damit unbefugte Zutritte zu identifizieren oder im Vorfeld zu verhindern (Abschreckung), kann es sich um eine technische Maßnahme i.S.d. Art. 32 DS-GVO handeln. Wird hingegen eine Überwachungskamera in einem Mitarbeiterbüro eingesetzt, um die Produktivität der

---

<sup>32</sup> Allgemein finden sich Ansätze dahingehend, dass die Sicherheit der Verarbeitung anderen datenschutzrechtlichen Prinzipien entgegenstehen kann, bei: Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 1b, 59a; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 11; v. *Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 41 ff. Siehe auch nicht nur auf Art. 32 DS-GVO beschränkt, sondern allgemein auf die Sicherheit von Informationssystemen und Informationen: Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 2, 33 ff.; *Schulte/Wambach*, DuD 2020, S. 462 ff.; Hornung/Schallbruch/*Jandt*, IT-Sicherheitsrecht, 2021, § 17, Rn. 48 ff.; Leupold/Wiebe/Glossner/*Leupold/v.d. Bussche/Schelinski*, IT-Recht, 4. Auflage 2021, Teil 7.1., Rn. 130; Taeger/Pohle/*Deusch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 303 (Stand: Mai 2022); DSK, Standard-Datenschutzmodell, Version 3.0, S. 52, 55 f. Siehe auch Specht/Mantz/*Schneider*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 15, Rn. 30, hinsichtlich eines (hier weniger relevanten Konflikts) zwischen Art. 32 DS-GVO und einer Löschungspflicht personenbezogener Daten, im Rahmen von Sicherungskopien. Siehe auch die Ausführungen bei *Hoeren*, NJW 2004, S. 3513 ff., wo – auf Basis der alten Rechtslage – im Rahmen von Virenskans und Spamfiltern immer mal wieder auch die Frage zwischen Datenschutz und Datensicherheit aufgeworfen wird.

<sup>33</sup> Vgl. Roßnagel/*Husemann*, Das neue Datenschutzrecht, 2018, § 5, Rn. 134, 152; Jandt/Steidle/*Richter*, Datenschutz im Internet, 2018, B. IV., Rn. 39; v. *Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 8; Freund u.a./*Freund/Schöning*, DSGVO, 2023, Art. 32 DS-GVO, Rn. 24. Siehe auch Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 28, spricht von „*normativen Anknüpfungspunkt*“.

Mitarbeiter zu überwachen, liegt hierin keine Maßnahme nach Art. 32 DS-GVO. Eine datenschutzrechtliche Bewertung solcher Maßnahmen muss daher differenzierter erfolgen. Bezogen auf das Beispiel der Überwachungskamera, können daher allgemeine datenschutzrechtliche Bewertungen oder Bewertungen zu anderen Einsatzzwecken nicht pauschal auf die Sicherheit der Verarbeitung übertragen werden.

Dieser Aspekt rechtfertigt aber nur noch mehr, sich einmal einige der in Frage kommenden Maßnahmen im Lichte beider Regelungsbereiche anzuschauen. Denn hierdurch könnten sich auch neue Wertungen in anderen Diskussionsbereichen ergeben.

## II. „Überwachungsmaßnahmen“ als Anwendungsfeld datenverarbeitender TOM

### 1. Allgemeines

Die praktische Bedeutung datenverarbeitender TOM und damit gleichzeitig sowohl ein besseres Verständnis über das Spannungsverhältnis als auch dessen Probleme lassen sich am besten anhand von einigen Beispielen aufzeigen. Die Darstellung des Problems anhand von Beispielen setzt jedoch zunächst ein grundlegendes Verständnis über den Inhalt der Sicherheit der Verarbeitung nach Art. 32 DS-GVO voraus. Die inhaltliche Aufbereitung ist allerdings auch Voraussetzung für eine Lösung datenverarbeitender TOM und soll daher an entsprechender Stelle ausführlicher erfolgen.<sup>34</sup> Eine ausführliche Auseinandersetzung dieses Punktes bereits im Rahmen der allgemeinen Problembeschreibung erscheint nicht geboten. Ein Vorgriff ist jedoch unausweichlich. Um diesen daher so gering wie möglich zu halten, beschränken sich die folgenden Ausführungen nur auf die wesentlichen Punkte, um die anschließenden Beispiele im Kontext des Untersuchungsgegenstands nachvollziehen zu können.

Einfach ausgedrückt umfasst die Sicherheit nach Art. 32 DS-GVO die Gewährleistung einer planmäßigen Verarbeitung personenbezogener Daten, um unerwünschte Vorfälle, wie bspw. die Zerstörung, Änderung oder Offenlegung von personenbezogenen Daten zu verhindern (vgl. Art. 32 Abs. 2 DS-GVO).<sup>35</sup>

---

<sup>34</sup> Siehe daher ausführlich: Teil 2, insbesondere Kapitel 4 und Kapitel 5.

<sup>35</sup> Siehe zur ausführlichen Herleitung des Regelungsziels des Art. 32 DS-GVO: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO*.

Um dieses Ziel zu verwirklichen, müssen technische und organisatorische Maßnahmen implementiert werden, die in der Lage sind, eine befugte von einer unbefugten Verarbeitung zu unterscheiden und im Falle einer unbefugten Verarbeitung diese zu verhindern. Mit diesem Ziel geht zwangsweise eine gewisse Form der Überwachung einher, um die verschiedenen Gefahren im Zusammenhang mit der Sicherheit der Verarbeitung abzudecken. Gleichzeitig eröffnet sich damit das Problem zur datenschutzrechtlichen Vorabkontrolle. Denn abhängig von ihrer jeweiligen Funktionsweise überwachen die TOM dabei auch natürliche Personen und dürften somit ihrerseits personenbezogene Daten dieser Personen verarbeiten (datenverarbeitende TOM).

## 2. Rollenkonzepte und Authentifizierungen

Die Sicherheit der Verarbeitung muss gewährleisten, dass nur befugte Personen auf die personenbezogenen Daten zugreifen können und von ihnen verarbeitet werden. Häufig werden daher Rollen- und Berechtigungskonzepte implementiert.<sup>36</sup>

Beispielsweise sollen Mitarbeiter der Personalabteilung keinen Zugriff auf die Kundendaten eines Unternehmens erhalten. Es liegt nicht im Aufgabenbereich der Personalabteilung, Kundendaten zu verarbeiten (Prinzip des „Need-to-know“)<sup>37</sup>. Sie sind daher schon im Grundsatz nicht befugt, auf diese Daten zuzugreifen. Abhängig von der jeweiligen Betrachtungsebene lassen sich diese

---

<sup>36</sup> Siehe zu Rollen- und Berechtigungskonzepten im Rahmen des Art. 32 DS-GVO: Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 52; Forgó/Helfrich/Schneider/Schmieder, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 60; Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 20, 23, 25; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 39, „Berechtigungssysteme [...] mit einer Authentifizierung“; Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 96, 98. Siehe auch allgemein zur Sicherheit Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 51; vgl. auch Schläger/Thode/Schläger, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 306 ff., allgemein als TOM.

<sup>37</sup> Knyrim/Pollirer, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.27, zum Punkt „Zugriffskontrolle“; ähnlich Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 25; Wächter, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 745; Katko/Meyer, Checklisten zur Datenschutz-Grundverordnung, 2. Aufl. 2023, § 9, Rn. 56 ff.; Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 19b, allgemein zu dem Ziel „Vertraulichkeit“.

Bereiche weiter differenzieren. So muss vielleicht nicht jeder Mitarbeiter der Personalabteilung auf sämtliche Personaldaten zugreifen können, weshalb auf jeder weiteren Ebene Abstufung vorzunehmen sind.

Mit einem Rollenkonzept kann diese Trennung sichergestellt werden. Bei einem Rollenkonzept handelt es sich streng genommen nicht um eine konkrete technische oder organisatorische Maßnahme. Denn Rollenkonzepte lassen sich auf verschiedene Arten umsetzen. Das wesentliche Konzept dahinter ist im Grunde allerdings identisch. Es geht um die Zuteilung und den Umfang verschiedener Rechte wie Lese- oder Bearbeitungsrechte für bspw. einen Datenbestand (wie die Daten auf dem Unternehmensserver).<sup>38</sup> Personen, die auf den Datenbestand zugreifen, können daher nur diese Daten verarbeiten, für die sie entsprechende Rechte haben.

Damit ein solches Rollenkonzept funktioniert, müssen die zugreifenden Personen und der Umfang ihrer Befugnisse zunächst identifiziert und anschließend müssen ihnen die darauf gerichteten Rechte zugeteilt werden. Schließlich bedarf es dann noch der Identitätsüberprüfung. Denn die zugreifende Person muss sich gegenüber dem System oder der Einrichtung als befugte Person ausweisen. Im häufig genutzten Fall von Softwarelösungen handelt es sich hier meist um ein Benutzerkonto, bei dem sich die zugreifende Person mit ihrem Kontoname und persönlichem Passwort anmelden muss. Im Rahmen dieses ganzen Konzepts müssen daher für die Authentifizierung berechtigter Personen die personenbezogenen Daten dieser Personen verarbeitet und im Rollenkonzept hinterlegt werden.<sup>39</sup>

---

<sup>38</sup> Vgl. Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 52; Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 25; siehe auch Forgó/Helfrich/Schneider/Schmieder, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 60 f.; Wächter, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 745.

<sup>39</sup> Siehe allgemein zur Verarbeitung personenbezogener Daten in Rollen- bzw. Berechtigungskonzepten: Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 51; vgl. auch Wächter, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 743, am Beispiel von Ausweisleser für Zutrittskontrollen; siehe auch Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 7, bzgl. „Zugriffsrechteverwaltung“; vgl. auch die Beispiele bei Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 34.

Nun mag das Erfassen berechtigter Personen und die Hinterlegung eines (hoffentlich abstrakten) Passworts noch nicht als bedenkliche Datenverarbeitung anzusehen sein, bei der tiefe Eingriffe in die datenschutzrechtlichen Interessen der betroffenen Person zu erwarten sind. Zum Schutz vor unbefugten Zugriffen, insbesondere durch Missbrauch, kann die Datenverarbeitung aber auch umfassender ausfallen. Zur Authentifizierung können Systeme scheinbar auch eine Geolokalisierung verwenden, um einen berechtigten von einem unberechtigten Zugriff zu unterscheiden. Dabei überprüft das System, von welchen Orten sich die berechnete Person in das System einloggt.

*Aus dem Alltag dürfte man diesen Fall vielleicht kennen, wenn bspw. die Logins in ein Konto über die, in diesem Konto hinterlegte E-Mail-Adresse gemeldet werden. In der E-Mail wird der Kontoeigentümer über den Login informiert und soll überprüfen, ob dieser Zugriff berechtigt war. Dabei finden sich meist auch Angaben wie der Ort<sup>40</sup>, die Zeit und welches Gerät für den Login verwendet wurde. Für den Fall eines unberechtigten Zugriffs findet sich in der E-Mail meist die Möglichkeit, das Konto zu sperren oder ein neues Passwort zu vergeben.*

Während in dem beschriebenen Beispiel die Kontrolle, ob es sich um einen berechtigten oder unberechtigten Zugriff handelt, dem betroffenen Nutzer obliegt, könnte aber auch systemseitig eine Analyse vorgenommen werden. Bspw. könnte das System feststellen, dass ein Zugriff von einem gänzlich anderen Ort (bspw. sogar aus einem anderen Land) erfolgte. Dies könnte den Verdacht eines missbräuchlichen Zugriffs nahelegen. Das System könnte dann so programmiert sein, dass es die Anfrage blockiert und ggf. weitere Identitätsnachweise fordert, um einen berechtigten Zugriff nachzuweisen.<sup>41</sup> Hiermit ließe sich die Gefahr begegnen, dass die persönlichen Authentifizierungsdaten durch einen unbefugten Dritten abgefangen oder sonst zur Kenntnis gelangt wurden.

Dieses Beispiel zeigt, dass im Rahmen solcher Authentifizierungsprozesse, die Teil eines Rollenkonzepts sein können, auch deutlich umfassendere Daten

---

<sup>40</sup> Meist dürfte es sich hierbei nur um ungefähre Ortsangaben handeln.

<sup>41</sup> Ein ähnlicher Fall ist dem Autor passiert. Ein Dienstanbieter hat ihn über einen Login-Versuch unterrichtet, der als Verdachtsfall eingeordnet und vorläufig blockiert wurde. Die Angaben erweckten den Eindruck, dass die Einstufung als Verdachtsfall u.a. deshalb erfolgte, da der Zugriff aus einem anderen Land kam. Ob die unberechtigte Person dabei aber tatsächlich auch über die vollständigen Zugangsdaten verfügte, ging aus der Information nicht hervor.

verarbeitet werden können. Neben einem Abgleich der Zugriffsorte könnten solche Systeme auch nach Tageszeiten (bspw. außerhalb von Arbeitszeiten), verwendeten Endgeräten oder einer Kombination mehrere Aspekte konfiguriert werden.

### 3. Logfiles und andere Dokumentationen

Eng mit dem Konzept der Rollen- und Rechteverteilung verbunden, ist die Dokumentation der Verarbeitung. Maßnahmen wie eine Authentifizierung schützen nicht vollumfänglich und können umgangen oder missbraucht werden. Daher ist es auch von Bedeutung, einen Missbrauch oder ein Fehlverhalten im Nachhinein aufzudecken.<sup>42</sup> Hierzu dient u.a. die Dokumentation, welche Personen wann auf personenbezogene Daten zugegriffen haben und welche Verarbeitungen vorgenommen wurden. Hiermit kann überprüft werden, welche Aktivitäten berechtigt waren und welche nicht. Die Überwachung der Zugriffe können dabei u.a. mittels Logfiles erfolgen, in denen jeder Zugriff bspw. von welcher Person, zu welcher Zeit und der betroffene Datensatz, gespeichert werden.<sup>43</sup>

---

<sup>42</sup> Weth u.a./*Overkamp/Overkamp*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 33; Forgó/Helfrich/Schneider/*Schmieder*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 75 ff.; *Wächter*, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 747. Siehe auch Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 5, der in der Nachprüfbarkeit unter dem Stichwort der „*Revisionsfähigkeit bzw. Revisionssicherheit*“ ein wesentliches Schutzziel sieht.

<sup>43</sup> Vgl. *Schulte/Wambach*, DuD 2020, S. 462, 464; Hornung/Schallbruch/*Jandt*, IT-Sicherheitsrecht, 2021, § 17, Rn. 49, allgemein zur „*IT-Sicherheit*“; Sassenberg/Faber/*Mantz/Spittka*, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 176 auch allgemein zur „*IT-Sicherheit*“; *Schläger/Thode/Schläger*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 316 ff., allgemein zur Protokollierung als TOM. Siehe allgemein zur Nachprüfbarkeit auch *Wächter*, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 747, als Anforderung im Rahmen der „*Eingabekontrolle*“ sicherzustellen, wer auf welche Daten zugegriffen hat; ähnlich Forgó/Helfrich/Schneider/*Schmieder*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 75 ff.; ebenso Weth u.a./*Overkamp/Overkamp*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 33; auch allgemein in diese Richtung Knyrim/*Pollner*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.27, ebenfalls unter dem Begriff „*Eingabekontrolle*“ mit Maßnahmen wie „*Protokollierung*“; Moos/Schefzig/*Arning/Heinemann*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 98, „*Protokollierung von Schreib-, Lösch- und Änderungszugriffen*“.



Besteht der Verdacht einer Sicherheitsverletzung, können diese Dokumentationen dabei helfen, die Verletzungen und ihre Ursachen zu identifizieren, rückgängig zu machen und mögliche Schwachstellen für die Zukunft zu beseitigen. Die Dokumentation der Verarbeitung umfasst dabei zwangsweise personenbezogene Daten derer, die an der Verarbeitung beteiligt sind.<sup>44</sup>

#### 4. Daten-Backups

Das Beispiel von Daten-Backups als (kritischer) Anwendungsbereich von datenverarbeitenden TOM wirkt zunächst eigenartig. Ein Backup ist eine Kopie eines Datenbestands, die getrennt vom ursprünglichen Datenbestand des „Live-Systems“ aufbewahrt wird.<sup>45</sup> Im Kontext der Sicherheit der Verarbeitung können Backups eingesetzt werden, um eine unplanmäßige Datenverarbeitung rückgängig zu machen, indem man den alten Datenbestand wiederherstellt.<sup>46</sup> Der Einsatz von Backups wird scheinbar auch gezielt von Art. 32 Abs. 1 Hs. 2 lit. c) DS-GVO befürwortet.<sup>47</sup>

---

<sup>44</sup> Siehe Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 5, 7, allgemein zur „Protokollierung von Zugriffen und Eingaben“; auch Forgó/Helfrich/Schneider/Schmieder, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 76 f.; ebenso Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 33; Sassenberg/Faber/Mantz/Spitka, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 176, „personenbezogene Protokollierungen“. Siehe zur Verarbeitung von personenbezogenen Daten durch File Logging Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 59a; Schulte/Wambach, DuD 2020, S. 462, 464 f.; Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 49; Thüsing/Thüsing/Traut, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 9, Rn. 19 ff., am Beispiel von E-Mail-Logfiles.

<sup>45</sup> Vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 38a; Leupold/Wiebe/Glossner/Leupold/Wiebe/Glossner, IT-Recht, 4. Auflage 2021, Begriffserklärung, Begriff: „Back-up“.

<sup>46</sup> Schläger/Thode/Meyer/T. Schmidt, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 49 f.; vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 41c i.V.m. Rn. 41 ff.

<sup>47</sup> Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 70; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 41c i.V.m. Rn. 38a, 41c; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 21; Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 41. Siehe auch Schläger/Thode/Meyer/T. Schmidt,

Dass mit Backups eine Verarbeitung personenbezogener Daten verbunden ist, dürfte offensichtlich sein, da es sich schließlich um eine Kopie der ursprünglichen (hier personenbezogenen) Daten handelt. Fraglich ist aber, was Backups und die damit verbundene Datenverarbeitung als geeignetes Beispiel für das Problem datenverarbeitender TOM ausmacht. Denn man könnte die Ansicht vertreten, dass es sich ja nur um eine Kopie, der bereits zu verarbeitenden Daten handelt.

Durch Backups tritt jedoch ein weiterer Kontrollverlust für die betroffenen Personen ein, da ihre Daten dadurch an einer weiteren Stelle verarbeitet werden. Gefahren können sich dann daraus ergeben, dass die Daten einem größeren Kreis von Personen bekannt werden könnten oder sogar – entgegen den verfolgten Zielen – ein unbefugter Zugriff auf die Daten erleichtert werden könnte, wenn die Backups nicht ausreichend geschützt werden.<sup>48</sup> Auffällig ist hier am Beispiel der Backups, dass es auch datenverarbeitende TOM gibt, bei denen die von ihnen betroffenen Personen identisch sein könnten mit den Personen, die nach Art. 32 DS-GVO zu schützen sind.

### 5. Überwachung von Datenkanälen

Als abschließendes Beispiel sollen noch Maßnahmen zur Überwachung von Datenkanälen Erwähnung finden. Die unbefugte Weitergabe personenbezogener Daten, sei es durch deren Offenlegung oder die Verschaffung eines Zugangs zu diesen Daten, stellt ebenfalls eine Gefahr für die Sicherheit der Verarbeitung dar (vgl. auch Art. 32 Abs. 2 DS-GVO).<sup>49</sup> Um dieser Gefahr zu begegnen, kann es sinnvoll sein, Datenkanäle zu überwachen, um einen Abfluss personenbezogener Daten zu verhindern.

---

Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 49, aber mit einem (wohl versehentlichen) Verweis auf „Art. 32 Abs. 1 lit. d DSGVO“.

<sup>48</sup> Vgl. Schläger/Thode/Meyer/T. Schmidt, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 64; Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 41, mit dem Hinweis, dass Backups ebenfalls nach Art. 32 DS-GVO zu schützen sind. Siehe hierzu auch Heidrich, Stresstest für die DSGVO, in: Den Wandel begleiten, 2020, S. 391, 394 f., der eine Datenpanne beschreibt, bei der aufgrund eines Fehlers Backup-Daten öffentlich verfügbar waren.

<sup>49</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 34; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 54; Gierschmann u.a./Jergl, Datenschutz-Grundverordnung, 2018, Art. 32 DS-GVO, Rn. 39.

Ein Beispielsfall könnte die Überwachung des E-Mail-Verkehrs sein. Häufig werden personenbezogene Daten per E-Mail übermittelt, wie z.B. Kundendaten. Problematisch wird es allerdings, wenn die personenbezogenen Daten entweder unbefugt übermittelt werden oder an die falsche Person übermittelt werden. Um dieser Gefahr zu begegnen, könnten die Übermittlungskanäle überwacht werden.

Im Falle von E-Mails könnte man überlegen, dass bestimmte E-Mails erst durch den Vorgesetzten oder einer anderen Stelle genehmigt werden müssen (4-Augen-Prinzip)<sup>50</sup>, bevor sie verschickt werden. Durch die stetige (Weiter-)Entwicklung von KI-Systemen können aber auch automatisierte Lösungen denkbar sein. So bieten bereits jetzt schon Softwarelösungen die Überprüfung von E-Mails an, bevor diese final an den Empfänger verschickt werden.<sup>51</sup> Dabei dürfen die E-Mails auf bestimmte Inhalte überprüft werden können, die vorab in einer „Blacklist“ definiert wurden.<sup>52</sup> Enthält die E-Mail „verbotene“ Inhalte, dann kann das System den Versand blockieren und ggf. den Absender oder eine andere Stelle benachrichtigen, die den Inhalt überprüft.<sup>53</sup> Diese Maßnahmen dürften zwar meist zum Schutz von Geschäftsgeheimnissen angewandt werden,

---

<sup>50</sup> Siehe allgemein zum 4-Augen-Prinzip im Rahmen des Art. 32 DS-GVO: *Gärtner/Selzer*, DuD 2023, S. 289, 290. Vgl. auch *Schlegel*, ZD 2020, S. 243, 243, allerdings in Verbindung mit einem Verstoß gegen die Vorgaben im Rahmen einer „Data-Loss-Prevention(DLP)-Software“ und damit wohl erst bei einem Verdachtsfall.

<sup>51</sup> *Schlegel*, ZD 2020, S. 243, 243, zu sog. „Data-Loss-Prevention(DLP)-Software“; auch zu Data-Loss-Prevention Systemen *Auer-Reinsdorff/Conrad/Conrad/Treger*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 293; vgl. *Schläger/Thode/Borchers*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel C, Rn. 315, will im genannten Beispiel zur Kartellrechts-Compliance aus Gründen der Verhältnismäßigkeit die Prüfung aber nur auf den Posteingang beschränken.

<sup>52</sup> *Schlegel*, ZD 2020, S. 243, 243, Vergleich mit der „DLP-Policy“ im Rahmen einer „Data-Loss-Prevention(DLP)-Software“; auch hierzu *Auer-Reinsdorff/Conrad/Conrad/Treger*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 293; vgl. *Schläger/Thode/Borchers*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel C, Rn. 315, „Suchbegriffe“; *Hauschka/Moosmayer/Lösler/Schmidl*, Corporate Compliance, 3. Aufl. 2016, § 28, Rn. 325, 353, „Stichwörter“.

<sup>53</sup> Siehe *Schlegel*, ZD 2020, S. 243, 243 im Rahmen von „Data-Loss-Prevention(DLP)-Software“; vgl. auch zu diesen Systemen *Auer-Reinsdorff/Conrad/Conrad/Treger*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 293 und den dort genannten Funktionen, siehe zudem Rn. 295.

könnten aber auch für personenbezogene Daten denkbar sein.<sup>54</sup> Während viele Systeme wohl auf eine genaue Übereinstimmung mit den definierten, verbotenen Inhalten angewiesen sind, könnten durch die Entwicklung im KI-Bereich zukünftig auch komplexere Überprüfungen möglich sein.<sup>55</sup>

Egal ob die Überprüfung direkt von einem Menschen oder einer Maschine vorgenommen wird, werden bei dem Einsatz solcher Maßnahmen personenbezogene Daten verarbeitet.<sup>56</sup> Denn die Maßnahmen zielen darauf ab, den Inhalt der E-Mail aber auch damit verbundene Daten wie den Absender oder die Zeiten ihres Verfassens zu analysieren. Weiterhin werden E-Mails und E-Mail-Logfiles in der Regel auch gespeichert.<sup>57</sup> Sie können damit zudem eine Quelle sein, eine unbefugte Weitergabe von personenbezogenen Daten später zu identifizieren.<sup>58</sup>

Während die hier geschilderten Konstellationen der E-Mail-Überwachung eher darauf abzielen einen Datenabfluss von innen heraus zu verhindern, kann die Überwachung auch einen von außen organisierten Abfluss von Daten erfassen. Maßnahmen in diesem Bereich können sog. Angriffserkennungs- und -verhinderungssysteme (intrusion detection [und prevention] systems) sein.<sup>59</sup> Diese

---

<sup>54</sup> Schlegel, ZD 2020, S. 243, 243. Zum Einsatz des „E-Mail-Screening“ als Schutz von Geschäftsgeheimnissen: Hauschka/Moosmayer/Lösler/Schmidl, Corporate Compliance, 3. Aufl. 2016, § 28, Rn. 353. Siehe auch Schläger/Thode/Borchers, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel C, Rn. 312 ff., zum „E-Mail-Screening“ im Bereich von kartellrechtlichen Absprachen.

<sup>55</sup> Siehe bereits Auer-Reinsdorff/Conrad/Conrad/Treeger, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 293, die nicht nur auf „einfaches Keyword Matching“ abstellen, sondern auch „linguistische Analysefunktionalitäten“ ansprechen.

<sup>56</sup> Siehe Schlegel, ZD 2020, S. 243 ff. zur datenschutzrechtlichen Rechtmäßigkeit von „Data-Loss-Prevention(DLP)-Software“; ebenfalls mit dem Hinweis auf datenschutzrechtliche Probleme dieser Systeme Auer-Reinsdorff/Conrad/Conrad/Treeger, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 34, Rn. 294; siehe auch Schläger/Thode/Borchers, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel C, Rn. 312 ff. im Kapitel „Verarbeitung von Beschäftigten-daten“; siehe auch zur Verarbeitung personenbezogener Daten beim „E-Mail-Screening“ Hauschka/Moosmayer/Lösler/Schmidl, Corporate Compliance, 3. Aufl. 2016, § 28, Rn. 354.

<sup>57</sup> Siehe zur Speicherung von E-Mails gerade auch im Zusammenhang der Datensicherung nach Art. 32 DS-GVO Schläger/Thode/Meyer/T. Schmidt, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 53.

<sup>58</sup> Siehe hierzu bereits: Kap. 2, C., II., 3. Logfiles und andere Dokumentationen.

<sup>59</sup> Siehe zum Einsatz solcher Systeme im Zusammenhang mit Art. 32 DS-GVO: Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn.

dienen bspw. dazu eine Verbindung zu den Systemen (bspw. eine Internetverbindung) auf auffällige Aktivitäten, wie Zugriffsversuche, zu überwachen.<sup>60</sup> Sie stehen damit in einer engen Verbindung zu den Rollenkonzepten und dem bereits oben beschriebenen Beispiel.<sup>61</sup>

Als hiermit verwandte Maßnahmen können auch „E-Mail Protection Systeme“<sup>62</sup> angesehen werden. Der Schutzzumfang solcher Systeme kann unterschiedlich groß sein.<sup>63</sup> Umfasst sein können bspw. ein Malware-Schutz und ein Schutz vor Spams.<sup>64</sup> Im Rahmen des Spam-Schutzes werden i.d.R. Absender

---

45; u.a. zu Art. 32 DS-GVO *Krügel*, MMR 2017, S. 795 ff. und der Frage, ob ihr Einsatz datenschutzrechtlich zulässig ist; siehe auch *Deusch/Eggendorfer*, Intrusion Detection und DSGVO, in: Rechtsfragen digitaler Transformationen, 2018, S. 741 ff., im Zusammenhang mit Art. 24, 33 DS-GVO und später (S. 748) auch mit Verweis auf Art. 32 DS-GVO. Siehe allgemein zu diesen Systemen: *Taeger/Pohle/Deusch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 220 ff. (Stand: Februar 2021); *Wendzel*, IT-Sicherheit für TCP/IP- und IoT-Netzwerke, 2021, S. 206 ff.; *Schläger/Thode/Cyl*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 241 f.; *Kipker/Sobr/Kemmerich*, Cybersecurity, 2. Aufl. 2023, Kapitel 3, Rn. 198 ff.

<sup>60</sup> Vgl. *Schläger/Thode/Cyl*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 241 f.; *Taeger/Pohle/Deusch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 221 (Stand: Februar 2021), „*Network Intrusion Detection Systems*“; auch in *Deusch/Eggendorfer*, Intrusion Detection und DSGVO, in: Rechtsfragen digitaler Transformationen, 2018, S. 741, 742 ff.; *Kipker/Sobr/Kemmerich*, Cybersecurity, 2. Aufl. 2023, Kapitel 3, Rn. 198 ff., 203 ff., 206 ff.; siehe auch *Haas/Kast*, ZD 2015, S. 72 ff., wohl unter einer Art Oberbegriff „*Network Security Monitoring*“ und mit einer (datenschutz-)rechtlichen Bewertung (Rechtslage vor der Datenschutz-Grundverordnung).

<sup>61</sup> Siehe bereits: Kap. 2, C., II., 2. *Rollenkonzepte und Authentifizierungen*.

<sup>62</sup> Siehe allgemein zu diesen Systemen: *Auer-Reinsdorff/Conrad/Schmidt/Pruß*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 3, Rn. 308 ff. Siehe auch zur Absicherung eines Mailervers *Schläger/Thode/Klein-Henning*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 222.

<sup>63</sup> *Auer-Reinsdorff/Conrad/Schmidt/Pruß*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 3, Rn. 309, 311.

<sup>64</sup> *Auer-Reinsdorff/Conrad/Schmidt/Pruß*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 3, Rn. 309. Siehe auch zum Schutz vor Malware und Spams im Rahmen des Art. 32 DS-GVO *DatKomm/Polliver*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 45; ähnlich *Moos/Schefzig/Arning/Heinemann*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 96, 98, 101, zum „*Virenschutz*“; siehe *Schläger/Thode/Klein-Henning*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 222, generell als TOM; *Taeger/Pohle/Deusch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 328 (Stand:

und Inhalt einer E-Mail auf mögliche Anzeichen überprüft.<sup>65</sup> Der Malware-Schutz überprüft hingegen meist die Anhänge einer E-Mail auf mögliche Schadcodes.<sup>66</sup> Erkennen diese Systeme einen möglichen Angriff von Außen, können sie die E-Mail (oder ggf. nur betroffene Anhänge) unmittelbar löschen, in einen Quarantänebereich verschieben oder als potenziell gefährlich kennzeichnen.<sup>67</sup> Abhängig von dem jeweiligen Schutzzumfang dieser Systeme und ihrer Konfiguration können insbesondere durch die Analyse der Absenderdaten aber auch der E-Mail-Inhalte eine Vielzahl von personenbezogenen Daten umfasst sein.

### III. Zwischenergebnis

Obwohl das Spannungsverhältnis zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle in der derzeitigen Diskussion wohl eher nur oberflächlich behandelt wird, zeigt sich anhand der Beispiele, dass datenverarbeitende TOM keine Ausnahmereischeinungen darstellen. Denn ein wesentlicher Aspekt bei der Sicherheit der Verarbeitung ist die Überwachung der zu schützenden Verarbeitung, um einen planmäßigen Ablauf zu gewährleisten. Dabei zeigt sich allerdings, dass eine Überwachung der Verarbeitung häufig auch zu einer Überwachung der, an der Verarbeitung beteiligten Personen führen kann und hierbei im Rahmen der eingesetzten Maßnahmen personenbezogene Daten verarbeitet werden. Datenverarbeitende TOM leisten damit einen entscheidenden Beitrag zur Gewährleistung dieser Sicherheit und sind ein gängiges Mittel bei der Erfüllung ihrer Anforderungen. Aufgrund dieser hohen praktischen Relevanz dieser Maßnahmen ist eine Lösung für das beschriebene Spannungsverhältnis damit noch bedeutsamer.

---

Mai 2022), die E-Mail-Filterung auf Malware im Zusammenhang von TOM für die IT-Sicherheit und der damit einhergehenden Verarbeitung personenbezogener Daten anführen.

<sup>65</sup> Auer-Reinsdorff/Conrad/Schmidt/Pruß, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 3, Rn. 314; Heidrich/Tschoepe, MMR 2004, S. 75, 75; Hoeren, NJW 2004, S. 3513, 3515, jedenfalls unter dem damaligen Stand kritisch zur textbasierten Überprüfung aufgrund unzureichend klarer Filterbegriffe.

<sup>66</sup> Auer-Reinsdorff/Conrad/Schmidt/Pruß, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 3, Rn. 315 f.

<sup>67</sup> Auer-Reinsdorff/Conrad/Schmidt/Pruß, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 3, Rn. 314 ff.; Hoeren, NJW 2004, S. 3513, 3515 ff., will die Entscheidung über den weiteren Umgang mit Verdachtsfällen, wohl jedenfalls bei privaten Nutzern, diesen überlassen.

## Kapitel 3

### Gang der Darstellung

#### A. Probleme und Ziele der Arbeit

Das Spannungsverhältnis zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle im Zusammenhang mit datenverarbeitenden TOM droht zu einem Widerspruch innerhalb der Datenschutz-Grundverordnung zu führen. Zur Lösung wären drei Szenarien denkbar.

1. Art. 32 DS-GVO könnte die Vorgaben des Art. 6 DS-GVO „anerkennen“ und im Falle eines hieraus bestehenden Verbots datenverarbeitender TOM seinen eigenen Pflichtenumfang entsprechend anpassen.
2. Art. 6 DS-GVO könnte bei der Prüfung der Rechtmäßigkeit die Charakterisierung als Maßnahmen i.S.d. Art. 32 DS-GVO „privilegieren“ und die zugrundeliegende Datenverarbeitung erlauben.
3. Anstatt einer der beiden Vorschriften Vorrang vor der anderen zu gewähren, könnte es drittens auch zu einer Abwägung zwischen beiden Vorschriften kommen. Ähnlich wie nach dem, im deutschen Verfassungsrecht bekannten Prinzip der „*praktischen Konkordanz*“<sup>1</sup> könnte man versuchen, beide Vorschriften in Einklang zu bringen, um einen Widerspruch zu verhindern und dabei den Zielen beider Vorschriften gebührend Rechnung tragen.

---

<sup>1</sup> BVerfG, BVerfGE 28, S. 243, 261; BVerfG, BVerfGE 97, S. 169, Rn. 28; BVerfG, BVerfGE 134, S. 204, Rn. 68; BVerfG, BVerfGE 148, S. 267, Rn. 32; BVerfG, NJW 2022, 2677, Rn. 41. Aus der Literatur: *Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl. 1999, Rn. 72; *Schladebach*, Der Staat Vol. 53 (2014), S. 263 ff.; *Hufen*, Staats-

Welches Szenario die Basis für eine gerechte Lösung sein sollte, bedarf jedoch zunächst einer Untersuchung, wie sich das beschriebene Spannungsverhältnis überhaupt ausgestaltet. Hierzu ist es erstmal erforderlich, sich die betreffenden Vorschriften und deren Pflichtenumfang genauer anzuschauen. Dabei geht es nicht nur darum, die jeweiligen Anforderungen zu identifizieren, die die Vorschriften an die Normadressaten stellen. Im Fokus steht vor allem das ihnen zugrundeliegende System.

Bereits bei der ersten Betrachtung der Art. 32 und Art. 6 DS-GVO fällt auf, dass die Pflichten sehr abstrakt beschrieben werden. Ein hoher Abstraktionsgrad kann dabei sowohl Vor- als auch Nachteile mit sich bringen. Ein Nachteil liegt in der Rechtsunsicherheit. Vorteilhaft könnte es allerdings sein, wenn sich in der Abstraktheit der Vorschriften Instrumente finden lassen, mit denen das Problem datenverarbeitender TOM innerhalb der Anforderungen der jeweiligen Vorschriften berücksichtigt werden kann.

---

recht II, 10. Aufl. 2023, § 9, Rn. 31; Stern/Sodan/Möstl/*Guckelberger*, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III, 2. Aufl. 2022, § 84, Rn. 27; *Manssen*, Staatsrecht II, 19. Aufl. 2022, Rn. 187; *Cremer*, Praktische Konkordanz als grundrechtliche Kollisionsauflösungsregel, in: FS Jarass, 2015, S. 175 ff., kritisch zur praktischen Konkordanz als „*Kollisionsauflösungsregel*“. Siehe zum Verweis auf dieses Prinzip auch im europäischen Recht bei kollidierenden Interessen: *Riesenhuber/Pechstein/Drechsler*, Europäische Methodenlehre, 4. Aufl. 2021, § 7, Rn. 31, für die Auslegung des Primärrechts; *Hornung/Gilga*, CR 2020, S. 367, Rn. 37, 56, im Zusammenhang des europäischen Datenschutzrechts; auch zum europäischen Datenschutzrecht *Rofsnagel*, NJW 2019, S. 1, 3, konkret zum Ausgleich dort widerstreitender Grundrechte; auch zum Datenschutz *Jandt/Steidle/Ambrock*, Datenschutz im Internet, 2018, A. II., Rn. 45; siehe im Zusammenhang des europäischen Wettbewerbsrechts: *Mestmäcker/Schweitzer*, Europäisches Wettbewerbsrecht, 3. Aufl. 2014, § 4, Rn. 135; siehe auch *Schweitzer*, Die Bedeutung nicht-wettbewerblcher Aspekte für die Auslegung von Art. 101 AEUV im Lichte der Querschnittsklauseln, in: Politischer Einfluss auf Wettbewerbsentscheidungen, 2015, S. 21, 24 f., 33 f.; *Immenga/Mestmäcker/Zimmer*, Wettbewerbsrecht, 1. Bd, 6. Aufl. 2019, Art. 101 Abs. 1 AEUV, Rn. 169 f.; siehe auch *Zimmer*, Begrüßung und Einführung: Wettbewerb und Politik – eine Einführung in das Thema, in: Politischer Einfluss auf Wettbewerbsentscheidungen, 2015, S. 8, 10, insb. mit weiteren Nachweisen in Fn. 10; *Dauses/Ludwigs/Hoffmann*, Hdb. des EU-Wirtschaftsrechts, Bd. 1, Stand: 59. EL. 2023, H., I., § 1, Rn. 6 (Stand: Juli 2019). Vgl. auch *Roth*, *RabelsZ* 75 (2011), S. 787, 840, der dafür plädiert, dass der EuGH bei seiner Rechtsfindung die Methodik offenlegen und begründen muss und nennt als Beispiel hier insbesondere auch die praktische Konkordanz. Siehe auch *GA Jacobs*, Schlussanträge v. 28.01.1999 zur Rs. C-67/96 (Albany), ECLI:EU:C:1999:28, Rn. 179, ohne das aber auf den Begriff der „*praktischen Konkordanz*“ abgestellt wird.



Denn das Ziel dieser Arbeit ist eine Lösung *de lege lata*. Hierfür bedarf es aber eine methodische Grundlage innerhalb der Vorschriften, an der man die Lösung ansetzen kann.

## B. Abgeleitete Forschungsfragen

Aus der Problemstellung lassen sich drei Forschungsfragen ableiten, die innerhalb dieser Arbeit beantwortet werden sollen:

1. Welche Folgen hat es auf die Sicherheit der Verarbeitung, wenn die Implementierung datenverarbeitender TOM an die Voraussetzungen einer rechtmäßigen Datenverarbeitung geknüpft werden und die Gefahr eines Verbots dieser Maßnahmen besteht?
2. Privilegiert die Klassifizierung als Maßnahme i.S.d. Sicherheit der Verarbeitung nach Art. 32 DS-GVO die Entscheidung über die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DS-GVO?
3. Wie sieht eine gerechte Lösung des Spannungsverhältnisses zwischen beiden Vorschriften unter Berücksichtigung der Ergebnisse zu den Fragen 1 und 2 aus?

Ausgangspunkt für die Antworten auf die Fragen ist die Sicherheit der Verarbeitung. Denn die Pflichten nach Art. 32 DS-GVO sind der Anlass zur Implementierung der problematischen Sicherheitsmaßnahmen. Daher sollten zunächst die Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO im Lichte datenverarbeitender TOM betrachtet werden. In einem weiteren Schritt gilt es dann zu prüfen, welchen Einfluss die Charakterisierung als Maßnahme i.S.d. Art. 32 DS-GVO auf die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten i.S.d. Art. 6 DS-GVO durch datenverarbeitende TOM haben kann. Die zweite Frage ist nicht zwingend an die Ergebnisse der ersten Frage gekoppelt und kann daher hiervon weitgehend isoliert betrachtet werden. Gemeinsam bilden die ersten beiden Fragen aber die Basis für die Lösung des Spannungsverhältnisses im Rahmen der 3. Frage.

## C. Themeneingrenzung

Bevor den Forschungsfragen im Einzelnen nachgegangen werden soll, bedarf es aber noch einer näheren Themeneingrenzung.

### *I. Betrachtung des Gesamtproblems*

Zunächst ist darauf hinzuweisen, dass in der Arbeit das Spannungsverhältnis im Zusammenhang datenverarbeitender TOM insgesamt untersucht werden soll. Dabei sollen die jeweiligen Probleme bezüglich der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle aufgezeigt und gelöst werden. Kein Ziel der Arbeit ist die rechtliche Bewertung individueller Maßnahmen.

### *II. Beschränkung auf den unternehmerischen Bereich*

Weiterhin soll sich die Untersuchung auf den privatwirtschaftlichen Bereich beschränken. Diese Eingrenzung ist nicht dahingehend zu verstehen, dass das Problem datenverarbeitender TOM für den öffentlichen Bereich nicht ebenfalls relevant wäre. Allerdings dürften die Gefahren hieraus für Unternehmen deutlich spürbarer sein. Dies gilt einmal für das drohende Haftungsrisiko, da gerade die behördlichen Bußgelder gegen öffentliche Stellen nur dann verhängt werden können, wenn die Mitgliedstaaten dies in ihrem nationalen Recht vorsehen (vgl. Art. 83 Abs. 7 DS-GVO) und bspw. Deutschland von dieser Möglichkeit keinen Gebrauch gemacht hat (vgl. § 43 Abs. 3 BDSG).<sup>2</sup>

Zum anderen dürfte im Zusammenhang mit der Sicherheit der Verarbeitung auch das Vertrauen betroffener Personen eine große Bedeutung spielen. Durch die zunehmende Sensibilisierung im Bereich des Datenschutzrechts dürften sich betroffene Personen mittlerweile genauer überlegen, wem sie ihre Daten anvertrauen. Anders als öffentliche Stellen, bei denen betroffene Personen es sich oftmals nicht aussuchen können, ob und welche personenbezogenen Daten von ihnen verarbeitet werden, müssen Unternehmen in vielen Bereichen Anreize schaffen und werben auch dafür, die Daten betroffener Personen zu verarbeiten. Dies könnte sich für Unternehmen mittelbar auf das Problem des Spannungsverhältnisses auswirken, wenn betroffenen Personen bspw. ein hohes

---

<sup>2</sup> Siehe hierzu bereits oben: Kap. 2, B., I. *Allgemeines Haftungsrisiko* (insb. Fn. 15).

Maß an Sicherheit<sup>3</sup> versprochen wird, das dann mit datenverarbeitenden TOM erreicht werden soll.

### III. Beschränkung auf die Datenschutz-Grundverordnung

Der untersuchte Rechtsrahmen beschränkt sich auf die Datenschutz-Grundverordnung. Das Datenschutzrecht wurde durch die Datenschutz-Grundverordnung europäisch weitgehend harmonisiert.<sup>4</sup> Die Verordnung stellt damit den ersten Anknüpfungspunkt für die datenschutzrechtliche Bewertung dar.<sup>5</sup> Im Rahmen sog. „Öffnungsklauseln“<sup>6</sup> kann jedoch nationales Recht zu beachten

---

<sup>3</sup> Siehe allgemein den Hinweis zur Möglichkeit des technischen und organisatorischen Datenschutzes als Wettbewerbsvorteil Laue/Kremer/Laue, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7 Rn. 1. Siehe ferner Hornung/Schallbruch/Bertschek/Janßen/Obnemus, IT-Sicherheitsrecht, 2021, § 3, Rn. 30 ff., allgemein zur „IT-Sicherheit als Wettbewerbsfaktor“, wobei aber auch gerade Wettbewerbsnachteile dargestellt werden.

<sup>4</sup> BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 1 DS-GVO (Stand: November 2021), Rn. 8; Hoeren/Sieber/Holznapel/Helfrich, Hdb. Multimedia-Recht, Stand: 59. EL. 2023, Teil 16.1, Rn. 22 ff. (Stand: August 2020); Ehmann/Selmayr/Selmayr/Ehmann, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung DS-GVO, Rn. 79 ff.; vgl. Simitis/Hornung/Spiecker gen. Döhmman/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Einleitung, Rn. 210 ff.

<sup>5</sup> Kühling, NJW 2017, S. 1985, 1986; Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 210; Taeger/Gabel/Taeger/Schmidt, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Einführung DS-GVO, Rn. 55; Paal/Pauly/Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Einleitung, Rn. 21; Leeb/Liebbaber, JuS 2018, S. 534, 536; vgl. auch Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 10 f.; Specht-Riemenschneider/Werry/Werry/Schmidt, Datenrecht in der Digitalisierung, 2020, § 2.1, Rn. 3, „Dreh- und Angelpunkt“.

<sup>6</sup> Siehe zum Begriff: Kühling/Martini, EuZW 2016, S. 448, 449; Kühling/Buchner/Kühling/Raab, DS-GVO – BDSG, 4. Aufl. 2024, A. Einführung, Rn. 98 ff.; Taeger/Gabel/Taeger/Schmidt, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Einführung DS-GVO, Rn. 51 ff.; Laue, ZD 2016, S. 463, 463; gegen die Verwendung des Begriffs Ehmann/Selmayr/Selmayr/Ehmann, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung DS-GVO, Rn. 89 und daher für die Bezeichnung „Spezifizierungsklausel“, u.a. in Anlehnung an ErwG 10 DS-GVO; ebenso mit Verwendung dieses Begriffs Hoeren/Sieber/Holznapel/Helfrich, Hdb. Multimedia-Recht, Stand: 59. EL. 2023, Teil 16.1, Rn. 22 (Stand: August 2020). Siehe auch ausführlicher zu den Öffnungsklauseln der Datenschutz-Grundverordnung: Kühling u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016; Jandt/Steidle/Ambrock, Datenschutz im Internet, 2018, A. II., Rn. 59 ff.

sein.<sup>7</sup> Nationales Recht soll aber so weit wie möglich aus der Untersuchung ausgeklammert werden.

Trotz dieser Öffnungsklauseln ist der Fokus auf die Datenschutz-Grundverordnung und das weitgehende Ausklammern nationalen Datenschutzrechts gerechtfertigt. Dies gilt auch für das Arbeitsrecht. Zwar enthält Art. 88 DS-GVO eine Öffnungsklausel, die es den Mitgliedstaaten gestattet, für Datenverarbeitungen im Beschäftigungskontext spezifischere Vorschriften zu erlassen. Wie die Beispiele zeigten,<sup>8</sup> dürften im Rahmen datenverarbeitender TOM oft auch personenbezogene Daten von Angestellten des Unternehmens verarbeitet werden. Daher wäre eine (nationale) Lösung im Beschäftigungskontext und in den Grenzen des Art. 88 DS-GVO zwar grds. denkbar. Das Spannungsverhältnis ist aber nicht zwingend auf den Beschäftigungskontext beschränkt. Daher erscheint eine Beschränkung auf diesen Bereich auch nicht angemessen. Zudem ist zu beachten, dass das hier dargestellte Problem im Kern des europäischen Datenschutzrechts verankert ist. Eine Lösung, die auf das Recht einzelner Mitgliedstaaten setzt, kann diesem Problem nicht gerecht werden. Es bedarf insofern einer europäischen Lösung, die losgelöst von nationalen Regelungsspielräumen funktioniert.

#### IV. Beschränkung auf den Pflichtbereich der Sicherheit der Verarbeitung

Die Gewährleistung einer hohen Sicherheit muss nicht zwingend eine gesetzliche Forderung an den Datenverarbeitern darstellen. So können gerade Unternehmen für hohe Sicherheitsstandards im Rahmen ihres Leistungsportfolios

---

<sup>7</sup> Die Datenschutz-Grundverordnung wird daher oft auch als eine Art Mischform zwischen Verordnung und Richtlinie eingeordnet: *Kühling/Martini*, EuZW 2016, S. 448, 449, „*Handlungsformenhybrid*“ und „*atypischer Hybrid*“; auch *Kühling/Buchner/Kühling/Raab*, DS-GVO – BDSG, 4. Aufl. 2024, A. Einführung, Rn. 98; *Kühling* u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 1, teilweise „*Richtlinie im Verordnungsgewand*“; ähnlich *Schulze/Janssen/Kadelbach/Holzengel/Felber*, Europarecht, 4. Aufl. 2020, § 38, Rn. 6; *Schneider*, Datenschutz, 2. Aufl. 2019, S. 46, „*Mittelding*“ / „*Zwitterlösung*“; *Buchholtz*, DÖV 2017, S. 837, 838, als „*hybride Struktur*“ und „*hinkende Harmonisierung*“, die sich dann zudem mit der Frage auseinandersetzt, welche Grundrechte in diesem Bereich gelten. Kritisch hierzu und allenfalls für die Einordnung als „*hinkende Verordnung*“ *Ehmann/Selmayr/Selmayr/Ehmann*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung DS-GVO, Rn. 88; zu dieser Einordnung auch *Jabnel/Pallwein-Prettner*, Datenschutzrecht, 3. Aufl. 2021, S. 16.

<sup>8</sup> Siehe hierzu: Kap. 2, C., II. „*Überwachungsmaßnahmen als Anwendungsfeld datenverarbeitender TOM*“.

werben, um Kunden zu gewinnen.<sup>9</sup> Für einen echten Unique Selling Point (USP) müssen die Unternehmen dann über die gesetzlichen Anforderungen hinausgehen. Der Wunsch von Unternehmen, dieses freiwillige „Mehr“ an Sicherheit zu erbringen, kann zwar faktisch die Probleme im Rahmen des Spannungsverhältnisses weiter anfachen. Das freiwillige „Mehr“ an Sicherheit liegt allerdings nicht im Fokus der vorliegenden Arbeit und soll daher nicht ausführlich behandelt werden.<sup>10</sup> Der Schwerpunkt liegt in dem gesetzlich geforderten Bereich der Sicherheit der Verarbeitung und welche Auswirkungen es hat, wenn die Umsetzung in diesem Bereich im Falle datenverarbeitender TOM vor rechtliche Herausforderungen gestellt wird.

#### *V. Beschränkung auf die Rechtmäßigkeit der Verarbeitung nach Art. 6 DS-GVO*

Die rechtlichen Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten werden in dieser Arbeit zwar ausführlich behandelt.<sup>11</sup> Vorab ist allerdings darauf hinzuweisen, dass abhängig von den verarbeiteten Datenkategorien<sup>12</sup> auch unter der Datenschutz-Grundverordnung unterschiedliche Anforderungen an die rechtskonforme Verarbeitung gestellt werden. Besonders schützenswerte Daten wie „besondere Kategorien personenbezogener Daten“ i.S.d. Art. 9 Abs. 1 DS-GVO unterliegen dabei strengeren Anforderungen.<sup>13</sup>

---

<sup>9</sup> Siehe zur Sicherheit als möglichen Wettbewerbsvorteil bereits: Kap. 3, C., II. *Beschränkung auf den unternehmerischen Bereich* und dort insb. Fn. 3.

<sup>10</sup> Siehe hierzu lediglich die Ausführungen zur Möglichkeit einer Einwilligung als Rechtsgrundlage für diesen Bereich: Kap. 9, C., III., 4. *Denkbare Anwendungsfälle und Zwischenergebnis*.

<sup>11</sup> Siehe daher ausführlicher unten: Teil 3 *Die Rechtmäßigkeit datenverarbeitender TOM*.

<sup>12</sup> Siehe für die verschiedenen Datenkategorien in der Datenschutz-Grundverordnung: BeckOK Datenschutzrecht/*Schild*, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 4; Taeger/Gabel/*Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS.GVO, Rn. 3; *Matejek/Mäusezahl*, ZD 2019, S. 551, 551; Knyrim/*Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.49.

<sup>13</sup> Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 9 DS-GVO, Rn. 1; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 9 DS-GVO (Stand: August 2023), Rn. 1; Schantz/Wolff/*Schantz*, Das neue Datenschutzrecht, 2017, Rn. 700; Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 6, 159; *Franzen*, EuZA 2017, S. 313, 328.

Gerade die Daten nach Art. 9 Abs. 1 DS-GVO können dabei auch für datenverarbeitende TOM von Bedeutung sein. Man denke nur an Authentifizierungsmaßnahmen, die biometrische Merkmale (vgl. Art. 9 Abs. 1 DS-GVO i.V.m. Art. 4 Nr. 14 DS-GVO) wie den Fingerabdruck<sup>14</sup>, das Venenbild<sup>15</sup> oder das Irismuster<sup>16</sup> verwenden, um bspw. die Berechtigung zum Zugriff auf personenbezogene Daten zu überprüfen.<sup>17</sup>

<sup>14</sup> BeckOK Datenschutzrecht/*Schild*, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 140; Kramer/*Bongers*, IT-Arbeitsrecht, 3. Aufl. 2023, § 4, Rn. 169; *Byers/Winkler/Stelter*, NZA 2023, S. 457, 458; Taeger/*Gabel/Mester*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 9 DS-GVO, Rn. 14; Kühling/*Buchner/Weichert*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 14 DS-GVO, Rn. 4; *Schröder*, Datenschutzrecht für die Praxis, 5. Aufl. 2023, S. 119; Auer-Reinsdorff/*Conrad/Schmidt/Pruß*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 2, Rn. 498 f.; *Wächter*, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 739 f.; Weth u.a./*Kramer*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil B., VI., Rn. 2; Thüsing/*Thüsing/Granetzny*, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 13, Rn. 1; Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 34; Schläger/*Thode/Schirmmacher*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 194.

<sup>15</sup> BeckOK Datenschutzrecht/*Schild*, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 141a; Thüsing/*Thüsing/Granetzny*, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 13, Rn. 1; Schläger/*Thode/Schirmmacher*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 194; Kramer/*Bongers*, IT-Arbeitsrecht, 3. Aufl. 2023, § 4, Rn. 169 (Handgefäßstruktur); Weth u.a./*Kramer*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil B., VI., Rn. 2 (Handgefäßstruktur); Auer-Reinsdorff/*Conrad/Schmidt/Pruß*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 2, Rn. 498; Taeger/*Gabel/Mester*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 9 DS-GVO, Rn. 14 (Venenerkennung). Ausführlicher zu den technischen Verfahren *Uhl*, DuD 2020, S. 16 ff.

<sup>16</sup> Kramer/*Bongers*, IT-Arbeitsrecht, 3. Aufl. 2023, § 4, Rn. 169; *Schröder*, Datenschutzrecht für die Praxis, 5. Aufl. 2023, S. 119; Auer-Reinsdorff/*Conrad/Schmidt/Pruß*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 2, Rn. 498, 503; *Wächter*, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 739 f.; Weth u.a./*Kramer*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil B., VI., Rn. 2; Thüsing/*Thüsing/Granetzny*, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 13, Rn. 1; Schläger/*Thode/Schirmmacher*, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 194; Taeger/*Gabel/Mester*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 9 DS-GVO, Rn. 14 (Iriserkennung); auch *Byers/Winkler/Stelter*, NZA 2023, S. 457, 458; Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 34.

<sup>17</sup> Allgemein zum Nachweis der Berechtigung als Einsatzzweck: Kramer/*Bongers*, IT-Arbeitsrecht, 3. Aufl. 2023, § 4, Rn. 174 ff.; *Byers/Winkler/Stelter*, NZA 2023, S. 457, 458;

Welche Anforderungen die Verordnung an die Verarbeitung dieser sensiblen Daten stellt, eröffnet ein zusätzliches Problem des Verhältnisses zwischen den besonderen und allgemeinen Regelungen.<sup>18</sup> Aus Gründen der Kapazität kann dieser Spezialfrage hier allerdings nicht nachgegangen werden.

Weiterhin scheint es auch angemessen, zunächst einen Lösungsvorschlag für das allgemeine Problem zu entwickeln, bevor man versucht, eine – wohl hierfür

---

*Schröder*, Datenschutzrecht für die Praxis, 5. Aufl. 2023, S. 119; Auer-Reinsdorff/Conrad/Schmidt/Pruß, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 2, Rn. 497 ff.; *Wächter*, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 738 ff.; Weth u.a./Kramer, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil B., VI., Rn. 6 f.; Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 34; Thüsing/Thüsing/Granetzny, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 13, Rn. 3; Schläger/Thode/Schirrmacher, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 194, zur Zutrittskontrolle.

<sup>18</sup> Derzeit umstritten ist das Verhältnis zwischen Art. 6 und Art. 9 DS-GVO. Nach einer Ansicht muss zusätzlich zu Art. 9 Abs. 2 DS-GVO auch eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO vorliegen: Kühling/Buchner/Weichert, DS-GVO – BDSG, 4. Aufl. 2024, Art. 9 DS-GVO, Rn. 4; *Robrahn/Bremert*, ZD 2018, S. 291, 295; *Golla/Hofmann/Bäcker*, DuD 2018, S. 89, 92 f., wonach aber einige Tatbestände des Art. 6 Abs. 1 durch die Tatbestände des Art. 9 Abs. 2 „*automatisch mit erfüllt*“ werden; *Matejek/Mäusezahl*, ZD 2019, S. 551, 554 f., wobei Art. 6 Abs. 1 DS-GVO ggf. modifiziert wird; *Hornung/Gilga*, CR 2020, S. 367, Rn. 40; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 9 DS-GVO (August 2023), Rn. 11, wonach Art. 9 den Art. 6 „*normativ überlagert, nicht aber verdrängt*“; *Jahnel/Pallwein-Prettner*, Datenschutzrecht, 3. Aufl. 2021, S. 85, „*doppelte bzw. implizite Prüfung von Art. 9 Abs. 2 und Art. 6 Abs. 1*“; Schwartmann u.a./*Jaspers/Mühlenbeck/Schwartmann*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 9 DS-GVO, Rn. 21, „*Zusammenschau der Anforderungen aus Art. 6 und 9*“; wohl auch *Piltz*, K&R 2016, S. 557, 567, „*nicht allein [...] nach Art. 6 Abs. 1 verarbeitet werden*“. Nach a.A. sperrt Art. 9 Abs. 2 DS-GVO als *lex specialis* die Anwendung von Art. 6 Abs. 1 DS-GVO: *Schneider/Schindler*, ZD 2018, S. 463, 465; *Taeger/Gabel/Mester*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 9 DS-GVO, Rn. 2; *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3, Rn. 58; *Wybitul/Pötters/Rauer*, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 54; vgl. auch mit allgemeinem Verweis des Art. 9 Abs. 2 DS-GVO als *lex specialis* zu Art. 6 Abs. 1 DS-GVO *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 370, 455; mit allgemeinem Verweis als *lex specialis* des Art. 9 DS-GVO *Chibanguza/Kuß/Steegé/Steegé/Kuß*, Künstliche Intelligenz, 2022, § 2, C., Rn. 31; auch *Schneider*, Datenschutz, 2. Aufl. 2019, S. 133, 145. Siehe jedoch jüngst EuGH, Rs. C-667/21 (Krankenversicherung Nordrhein), ECLI:EU:C:2023:1022 = BeckRS 2023, 36822, Rn. 78, dass eine Verarbeitung besonderer Kategorien personenbezogener Daten nicht nur die Anforderungen nach Art. 9 Abs. 2 DS-GVO erfüllen muss, sondern insb. auch die Voraussetzungen des Art. 6 Abs. 1 DS-GVO.

erforderliche – Differenzierung für Sonderprobleme im Lösungsansatz vorzunehmen. Um die Untersuchung damit erstmal nicht unnötig zu verkomplizieren, sollte man daher bei dem Grundfall der „gewöhnlichen personenbezogener Daten“<sup>19</sup> bleiben und die Untersuchung daher auf Art. 6 DS-GVO beschränken. Abhängig davon, wie sich das Endergebnis gestaltet, könnte man dann hierauf aufbauend anfangen, Sonderkonstellationen zu berücksichtigen und die Lösung gegebenenfalls anpassen.

---

<sup>19</sup> Zu diesem Begriff: *Matejek/Mäusezahl*, ZD 2019, S. 551 ff.; alternativ werden insb. auch Begriffe wie „allgemeine personenbezogene Daten“ (BeckOK Datenschutzrecht/*Schild*, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 4), „normale personenbezogene Daten“ (Moos/Schefzig/Arning/*Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 6) oder „einfache personenbezogene Daten“ (Paal/Pauly/*Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 9 DS-GVO, Rn. 1) verwendet.



## Teil 2

### Datenverarbeitende TOM im Lichte der Sicherheit der Verarbeitung

Ausgangspunkt des, im 1. Teil beschriebenen Spannungsverhältnisses bei datenverarbeitenden TOM sind die Pflichten des Art. 32 DS-GVO. Denn wie dieses Spannungsverhältnis im Detail ausgestaltet ist und wie ein daraus gegebenenfalls erwachsender Konflikt letztlich gelöst werden könnte, hängt zunächst im Wesentlichen davon ab, welche Anforderungen die Datenschutz-Grundverordnung an die Sicherheit der Verarbeitung stellt.

Klar scheint zunächst zu sein, dass nach Art. 32 Abs. 1 DS-GVO Datenverarbeiter technische und organisatorische Maßnahmen implementieren müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Kommt es dann im Rahmen dieser TOM zu einer Verarbeitung personenbezogener Daten, so dürfte das beschriebene Spannungsverhältnis mit der datenschutzrechtlichen Vorabkontrolle i.S.d. Art. 6 DS-GVO bestehen. Doch bereits der flüchtige Blick auf Art. 32 Abs. 1 DS-GVO zeigt schon, dass die Anforderungen an die Sicherheit der Verarbeitung sehr abstrakt beschrieben werden. Damit stellt sich die Frage, welche Auswirkungen dies auf das Spannungsverhältnis haben kann. Auf der Seite des Art. 32 DS-GVO gilt es daher genauer zu untersuchen, welche konkreten Anforderungen die Datenschutz-Grundverordnung an die Sicherheit der Verarbeitung im Allgemeinen und im Besonderen an die Implementierung der TOM stellt, um deren Auswirkungen auf datenverarbeitende TOM zu bewerten.

Eine erste Hürde könnte jedoch bereits in der Interpretation des Normtextes liegen. Denn auf den ersten Blick scheinen die Anforderungen an die Sicherheit der Verarbeitung, die daraus entstehenden Pflichten und die damit verfolgten Ziele nicht ganz eindeutig in Art. 32 DS-GVO zum Ausdruck zu kommen.<sup>1</sup> Dies könnte zu Missverständnissen über den Regelungsinhalt führen. Bevor die Anforderungen an die Sicherheit der Verarbeitung und deren Auswirkungen auf das Problem datenverarbeitender TOM im Detail analysiert werden können, soll daher ein grundlegendes Verständnis über den Regelungsinhalt und die Ziele der Vorschrift erarbeitet werden.

---

<sup>1</sup> Siehe zu einer ähnlichen Kritik *Schneider*, Datenschutz, 2. Aufl. 2019, S. 264 f.



## Kapitel 4

# Das allgemeine Regelungsziel des Art. 32 DS-GVO

### A. Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.

In der Literatur werden die Ziele des Art. 32 DS-GVO nach ganz herrschender Ansicht in der Gewährleistung der sog. „Datensicherheit“ gesehen.<sup>1</sup> Zu den wesentlichen Schutzziele der Datensicherheit gehören dabei die Integrität, Vertraulichkeit und Verfügbarkeit.<sup>2</sup> Eine flüchtige Analyse des Art. 32 DS-GVO

---

<sup>1</sup> BeckOK Datenschutzrecht/*Paulus*, Stand: 46. Ed. 2023, Art. 32 DS-GVO (Stand: November 2021), Einleitung (Vor Rn. 1); Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 1; Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 1; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 5, unter der Überschrift „Regelungsgegenstand: Datensicherheit“; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 1; Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 6; Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 843 ff.; Roßnagel/*Husemann*, Das neue Datenschutzrecht, 2018, § 5, Rn. 135; *Wybitul*, NJW 2020, S. 2577, Rn. 1; *Johannes/Geminn*, InTeR 2021, S. 140, 141; *Gärtner/Selzer*, DuD 2023, S. 289, 290; *Folkerts*, ZD 2023, S. 654, 654; *Frisse* u.a., BKR 2018, S. 177, 182; *Kuner/Bygrave/Docksey/Burton*, GDPR, 2020, p. 634, unter Verwendung des englischen Begriffs „data security“.

<sup>2</sup> Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 3; *Wybitul*, NJW 2020, S. 2577, Rn. 3; *Seufert*, ZD 2023, S. 256, 257; *Johannes/Geminn*, InTeR 2021, S. 140, 141, stellt zusätzlich noch auf die „Belastbarkeit der Systeme“ ab; ähnlich Sassenberg/*Faber/Mantz/Spittka*, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 147; siehe auch *Forgó/Helfrich/Schneider/Weber/Suter*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XV, Kapitel 5, Rn. 45, konkret zum Schweizer Recht. Andere stellen hier hingegen auf die Schutzziele der „Informationssicherheit“ ab: *Simitis/Hornung/Spiecker* gen. *Döhmman/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn.

scheint dieses Verständnis zu unterstützen, denn so zeigen sich bspw. in Art. 32 Abs. 1 Hs. 2 lit. b) DS-GVO Anlehnungen an diese Schutzziele.<sup>3</sup>

Ein weiterer Hinweis auf diese Verbindung findet sich im Datenschutzgrundsatz nach Art. 5 Abs. 1 lit. f) DS-GVO. Die allgemeinen Datenschutzgrundsätze des Art. 5 DS-GVO werden durch eine Vielzahl der Vorschriften der Datenschutz-Grundverordnung näher konkretisiert.<sup>4</sup> Darüber hinaus sollen sie

---

12, 38; Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 19b; Knyrim/*Pollirer*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.7; Auernhammer/*Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 33, „gebräuchlichen Ziele des Informationssicherheitsmanagements“; Moos/Schefzig/*Arning/Heinemann*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 93, „Grundwerte“; Schwartmann u.a./*Ritter*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 43; Paal/*Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 58. Mit Verweis auf die Ziele der „IT-Sicherheit“: Wybitul/*Schreiberbauer/Spittka*, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 32 DS-GVO, Rn. 11; Ehmann/*Selmayr/Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 8; ähnlich Roßnagel/*Husemann*, Das neue Datenschutzrecht, 2018, § 5, Rn. 133; *Schulte/Wambach*, DuD 2020, S. 462, 464; *Gossen/Schramm*, ZD 2017, S. 7, 13, wobei in diesem Zusammenhang gleichfalls auf die „Informationssicherheit“ verwiesen wird. Zum Problem einer möglichen Begriffsabgrenzung sogleich. Siehe allgemein zur Anknüpfung an diese Ziele, ohne Bezug zu dem Begriff „Datensicherheit“ *Feiler/Forgó*, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 32 DS-GVO, Rn. 1, 8.

<sup>3</sup> Schuster/*Grützmacher/Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 3; Laue/*Kremer/Laue*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7, Rn. 27; Spindler/*Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 13. Mit Verweis auf die „Informationssicherheit“: *Simitis/Hornung/Spiecker* gen. *Döhmman/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 38; Auernhammer/*Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 33; Paal/*Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 58; Schwartmann u.a./*Ritter*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 43; Knyrim/*Pollirer*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.7, wonach Art. 32 Abs. 1 Hs. 2 lit. b) DS-GVO diese um die „Belastbarkeit“ ergänzt. Unter Verweis auf die „IT-Sicherheit“: Ehmann/*Selmayr/Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 8; Kühling/*Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 22, wobei diese Ziele als „Grundbedingungen für die Datensicherheit“ gelten sollen; *Schulte/Wambach*, DuD 2020, S. 462, 464.

<sup>4</sup> Kühling/*Buchner/Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 1; Ehmann/*Selmayr/Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 6; Taeger/*Gabel/Voigt*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 5 DS-GVO, Rn. 5; Kipker/*Reusch/Ritter/Herbst*, Recht der Informationssicherheit, 2023, Datenschutz-Grund-

auch unmittelbare Geltung entfalten.<sup>5</sup> Denn ein Verstoß gegen die Datenschutzgrundsätze kann mit einem Bußgeld sanktioniert werden (vgl. Art. 83 Abs. 5 lit. a) DS-GVO).<sup>6</sup> Ihre unmittelbare Geltung und gleichzeitig ihre Konkretisierung durch spezifischere Vorschriften der Verordnung führen zu einem Konkurrenzverhältnis, das gerade auch bei der Bemessung eines Bußgelds zum Problem werden kann.<sup>7</sup> Das Konkurrenzverhältnis hat für die hier zu untersuchenden Fragen nur eine nachrangige Bedeutung und wird daher nicht weiter verfolgt.

Der Datenschutzgrundsatz nach Art. 5 Abs. 1 lit. f) DS-GVO steht in einer engen Verbindung zu Art. 32 DS-GVO. Dies lässt sich daran erkennen, dass Art. 5 Abs. 1 lit. f) DS-GVO auf die „Sicherheit“<sup>8</sup> der personenbezogenen Daten abstellt und damit Ähnlichkeiten sowohl mit der Überschrift von Art. 32 DS-

---

verordnung, Art. 5 DS-GVO, Rn. 1; Schulze/Janssen/Kadelbach/Holznel/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 15; vgl. Gola/Heckmann/Pötters, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 4, „allgemeine Strukturprinzipien“, die das Datenschutzrecht als einen „roten Faden durchweben“; Moos/Schefzig/Arning/Moos, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 4, Rn. 1; Breyer, DuD 2018, S. 311, 315; Jahnel/Jahnel, DSGVO, 2021, Art. 5 DS-GVO, Rn. 1.

<sup>5</sup> Kühling/Buchner/Herbst, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 1; BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 2; Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 5; Gola/Heckmann/Pötters, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 4; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 5 DS-GVO, Rn. 2; Jahnel/Jahnel, DSGVO, 2021, Art. 5 DS-GVO, Rn. 1; Schulze/Janssen/Kadelbach/Holznel/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 15; Breyer, DuD 2018, S. 311, 315, der wohl gerade deshalb eine „völlige Deckungsgleichheit“ mit einzelnen Vorschriften der Verordnung ablehnt, um den eigenständigen Charakter der Grundsätze zu erhalten.

<sup>6</sup> Kühling/Buchner/Herbst, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 2; Gola/Heckmann/Pötters, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 4; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 5 DS-GVO, Rn. 2, mit Verweis auf das Problem hinsichtlich des Bestimmtheitsgebots; ähnlich BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 3; auch Taeger/Gabel/Voigt, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 5 DS-GVO, Rn. 7.

<sup>7</sup> Siehe hierzu bereits oben: Kap. 2, B., I. *Allgemeines Haftungsrisiko*, Fn. 18.

<sup>8</sup> Englisch: „security“, Französisch: „sécurité“, Spanisch: „seguridad“, Italienisch: „sicurezza“, Niederländisch: „beveiliging“.

GVO „Sicherheit der Verarbeitung“<sup>9</sup> als auch der Überschrift des Abschnittes „Sicherheit personenbezogener Daten“<sup>10</sup>, in den Art. 32 DS-GVO eingegliedert ist, aufweist. Weiterhin verweist Art. 5 Abs. 1 lit. f) DS-GVO in gekürzter Form auf wesentliche Punkte, die sich auch in Art. 32 DS-GVO wiederfinden lassen. Art. 32 DS-GVO wird als Konkretisierung dieses Grundsatzes verstanden.<sup>11</sup> Die Verbindung mit dem Begriff der Datensicherheit ergibt sich in Art. 5 Abs. 1 lit. f) DS-GVO insbesondere aus dessen Klammerdefinition „Integrität und Vertraulichkeit“<sup>12</sup>. Mit ihr verweist die Verordnung auch hier (zumindest)<sup>13</sup> auf zwei der drei wesentlichen Schutzziele des hier betrachteten Verständnisses des Begriffs der Datensicherheit.<sup>14</sup>

<sup>9</sup> Englisch: „Security of processing“, Französisch: „Sécurité du traitement“, Spanisch: „Seguridad del tratamiento“, Italienisch: „Sicurezza del trattamento“, Niederländisch: „Beveiliging van de verwerking“.

<sup>10</sup> Englisch: „Security of personal data“, Französisch: „Sécurité des données à caractère personnel“, Spanisch: „Seguridad de los datos personales“, Italienisch: „Sicurezza dei dati personali“, Niederländisch: „Persoonsgegevensbeveiliging“.

<sup>11</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 1; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 1; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 1; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 43 DS-GVO, Rn. 1; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 5; Johannes/Geminn, InTeR 2021, S. 140, 141; Wybitul, NJW 2020, S. 2577, Rn. 3 f.; Jandt/Steidle/Richter, Datenschutz im Internet, 2018, B. IV., Rn. 36; John/Schaller, CR 2022, S. 156, 156.

<sup>12</sup> Englisch: „integrity and confidentiality“, Französisch: „intégrité et confidentialité“, Spanisch: „integridad y confidencialidad“, Italienisch: „integrità e riservatezza“, Niederländisch: „integriteit en vertrouwelijkheid“.

<sup>13</sup> Sprachlich umfasst der Grundsatz nach Art. 5 Abs. 1 lit. f) DS-GVO die „Verfügbarkeit“ (als drittes Schutzziel) zwar nicht, dennoch soll es vom Inhalt des Datenschutzgrundsatzes umfasst sein, siehe hierzu: Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 167; Feiler/Forgó, EU-DSGVO und DSGVO, 2. Aufl. 2022, Art. 5 DS-GVO, Rn. 21; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 12; Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 39.

<sup>14</sup> BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 35; vgl. allgemein Gola/Heckmann/Pöppers, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 29. Siehe auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 12, wobei sie auf den Begriff „Informationssicherheit“ abstellt. Zum Problem einer möglichen Begriffsabgrenzung sogleich.

Auch wenn damit die Verbindung des Art. 32 DS-GVO mit dem Begriff der Datensicherheit daher zunächst nicht fernliegt, so eignet sich der Verweis auf die Datensicherheit dennoch nicht zur Beschreibung der Regelungsziele des Art. 32 DS-GVO. Dies liegt einmal daran, dass der Begriff der „Datensicherheit“ im Vorschriftenteil der Datenschutz-Grundverordnung an keiner Stelle mit direktem Verweis auf Art. 32 DS-GVO<sup>15</sup> verwendet und schon gar nicht legal definiert wird. Lediglich in Erwägungsgrund 83 S. 3 DS-GVO wird im Zusammenhang mit Art. 32 DS-GVO von „*Datensicherheitsrisiken*“<sup>16</sup> gesprochen. Was die Verordnung aber genau unter diesem Begriff verstehen möchte, geht hieraus nicht vollends hervor.

Es verwundert daher auch nicht, wenn in der Literatur die Ziele von Art. 32 DS-GVO mit anderen Begriffen in Verbindung gebracht werden. Nicht selten findet man bspw. auch den Verweis auf den Begriff der „*Informationssicherheit*“.<sup>17</sup> Ein weiterer Begriff, der im Zusammenhang mit Art. 32 DS-GVO Verwendung findet, ist der Begriff der „*IT-Sicherheit*“.<sup>18</sup> Von einigen scheint dieser

---

<sup>15</sup> Erwähnung findet der Begriff in Art. 47 Abs. 2 lit. d) DS-GVO. Die anderen Sprachfassungen verwenden hier, Englisch: „*data security*“, Französisch: „*la sécurité des données*“, Spanisch: „*la seguridad de los datos*“, Italienisch: „*sicurezza dei dati*“, Niederländisch: „*gegevensbeveiliging*“.

<sup>16</sup> Englisch: „*data security risk*“, Französische: „*des risques pour la sécurité des données*“, Spanisch: „*el riesgo en relación con la seguridad de los datos*“, Italienisch: „*del rischio per la sicurezza dei dati*“, Niederländisch: „*de gegevensbeveiligingsrisico's*“.

<sup>17</sup> Knyrim/Pollirer, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.1 ff.; Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 4 f., 12; Gossen/Schramm, ZD 2017, S. 7, 13; Suwelack, ZD 2020, S. 561, 562; vgl. auch Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 2, wobei Art. 32 DS-GVO die Anforderungen aus der Informationssicherheit übernimmt; siehe auch *Wybitul*, NJW 2020, S. 2577, Rn. 3.

<sup>18</sup> Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 5, Rn. 9; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 3; Laue/Kremer/Laue, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7, Rn. 21; Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 60; Gossen/Schramm, ZD 2017, S. 7, 13; Folkerts, ZD 2023, S. 654, 654.

Begriff synonym mit Begriffen wie „*Datensicherheit*“<sup>19</sup> oder „*Informationssicherheit*“<sup>20</sup> verwendet zu werden. Andere sehen hierin ein zusätzliches Ziel des Art. 32 DS-GVO.<sup>21</sup>

Eine klare Zuweisung des Art. 32 DS-GVO zu Begriffen wie „*Datensicherheit*“, „*Informationssicherheit*“ oder „*IT-Sicherheit*“ dürfte damit eher die Frage aufwerfen, wie diese Begriffe voneinander abzugrenzen sind.<sup>22</sup> Die Ziele von Art. 32 DS-GVO dürften sich allerdings selbst mit einer klaren Begriffszuweisung jedenfalls nicht im Detail damit beschreiben lassen. Eine Begriffszuordnung eignet sich daher allenfalls für eine erste und grobe Einordnung. Die rechtlichen Details verlangen hingegen zwingend einer Ableitung aus der Datenschutz-Grundverordnung heraus.

<sup>19</sup> Wohl als Synonym zum Begriff „*Datensicherheit*“: *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 5, Rn. 9 im Vergleich zur Überschrift des Abschnitts „*Datensicherheitsmaßnahmen*“; *Wybitul*, NJW 2020, S. 2577, Rn. 1, 3, unter Verwendung des englischen Begriffs „*IT-Security*“; *Folkerts*, ZD 2023, S. 654, 654; *Freund u.a./Freund/Schöning*, DSGVO, 2023, Art. 32 DS-GVO, Rn. 21, wenn es um „*elektronische Datenverarbeitungen*“ geht; siehe auch *Schuster/Grützmaker/Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 8, dass die Begriffe in diesem Fall „*weitgehende Bedeutungs-gleichheit*“ haben.

<sup>20</sup> Wohl als Synonym zum Begriff „*Informationssicherheit*“: *Simitis/Hornung/Spiecker* gen. *Döhmman/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 12, 60; *Wybitul*, NJW 2020, S. 2577, Rn. 1, 3; *Gossen/Schramm*, ZD 2017, S. 7, 13; vgl. *Freund u.a./Freund/Schöning*, DSGVO, 2023, Art. 32 DS-GVO, Rn. 21, wohl jedenfalls wenn es um personenbezogene Daten geht.

<sup>21</sup> *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 3; *Laue/Kremer/Laue*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7, Rn. 21, siehe auch in *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 1.

<sup>22</sup> Siehe allgemein zu möglichen Begriffsabgrenzungen in den hier Betracht kommenden, verschiedenen Konstellationen: *Kipker/Kipker*, Cybersecurity, 2. Aufl. 2023, Kapitel 1, Rn. 4, zur Abgrenzung der Begriffe „*IT-Sicherheit*“, „*Informationssicherheit*“ und „*Datensicherheit*“; *Hornung/Schallbruch/Jandt*, IT-Sicherheitsrecht, 2021, § 17, Rn. 1 ff.; v. *Lewinski/Rüpk/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 23, 37 ff., Abgrenzung von Art. 32 DS-GVO und IT-Sicherheit; *Kipker/Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 1, Abgrenzung insb. zwischen „*Informationssicherheit*“ und „*Datensicherheit*“; *Knyrim/Pollirer*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.2, Abgrenzung zwischen „*Informationssicherheit*“ und „*Datensicherheit*“; *Moos/Schefzig/Arning/Heinemann*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 37 f., zu den Begriffen „*Datensicherheit*“, „*Informationssicherheit*“ und „*IT-Sicherheit*“.



## B. Schutz der Rechte und Freiheiten

Für die Bestimmung des Regelungsziels kommt dem Begriff „*ein dem Risiko angemessenes Schutzniveau*“<sup>23</sup> aus Art. 32 Abs. 1 DS-GVO eine besondere Bedeutung zu. Denn nach dem Wortlaut soll es gerade dieses Schutzniveau sein, dass Datenverarbeiter mittels technischer und organisatorischer Maßnahmen gewährleisten sollen. Doch bereits in diesem Zusammenhang dürfte Art. 32 DS-GVO dem Rechtsanwender die Auslegung gleich auf zwei Weisen erschweren.

### I. Der Begriff des „Schutzniveaus“

Ausgehend von der Überschrift „*Sicherheit der Verarbeitung*“<sup>24</sup> des Art. 32 DS-GVO sollte man erwarten dürfen, dass im Rahmen der Vorschrift näher definiert wird, was unter der Sicherheit der Verarbeitung oder allgemein der Sicherheit im datenschutzrechtlichen Kontext zu verstehen ist. An einer solchen Definition oder einer weitergehenden, klaren Erklärung fehlt es in Art. 32 DS-GVO scheinbar. Denn stellt man zunächst nur auf die deutsche Sprachfassung ab, wird der Begriff „*Sicherheit*“ in der Vorschrift nur an einer einzigen – für dessen Auslegung aber eher unbedeutenderen –<sup>25</sup> Stelle im Normtext verwendet. Dafür stellt Art. 32 Abs. 1 DS-GVO fortan auf ein *Schutzniveau* ab.<sup>26</sup>

Warum Art. 32 DS-GVO nunmehr von einem Schutzniveau spricht und nicht weiter den Begriff der Sicherheit verwendet, verwundert. Damit stellt sich auch die Frage, ob dies Auswirkungen auf die Gesetzesauslegung hat und es somit einer Differenzierung zwischen beiden Begriffen bedarf. Das Erfordernis einer Abgrenzung legt ebenfalls ein erneuter Blick auf den Datenschutzgrundsatz

---

<sup>23</sup> Englisch: „*a level of security appropriate to the risk*“, Französisch: „*un niveau de sécurité adapté au risque*“, Spanisch: „*un nivel de seguridad adecuado al riesgo*“, Italienisch: „*un livello di sicurezza adeguato al rischio*“, Niederländisch: „*een op het risico afgestemd beveiligingsniveau*“.

<sup>24</sup> Englisch: „*Security of processing*“, Französisch: „*Sécurité du traitement*“, Spanisch: „*Seguridad del tratamiento*“, Italienisch: „*Sicurezza del trattamento*“, Niederländisch: „*Beveiliging van de verwerking*“.

<sup>25</sup> Der Begriff „*Sicherheit*“ wird in Art. 32 Abs. 1 Hs. 2 lit. d) DS-GVO noch einmal im Kontext der „*Sicherheit der Verarbeitung*“ aufgegriffen. Dabei scheint die Vorschrift auf sich selbst zu verweisen, ohne jedoch näher darauf einzugehen, was unter diesem Begriff zu verstehen ist.

<sup>26</sup> Feiler/Forgó, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 32 DS-GVO, Rn. 7, weisen ebenfalls auf diesen sprachlichen Aspekt hin.

nach Art. 5 Abs. 1 lit. f) DS-GVO nahe. Denn trotz ihrer Verwandtschaft<sup>27</sup> spricht Art. 5 Abs. 1 lit. f) DS-GVO von einer „*angemessenen Sicherheit*“. Auf den ersten Blick scheint die Verordnung hier in einem ähnlichen Kontext zwei unterschiedliche Begriffe zu verwenden. Eine abweichende Auslegung aufgrund der Anknüpfung an den Begriff des Schutzniveaus dürfte vom Gesetzgeber aber dennoch nicht gewollt sein. Dies geht aus einem Vergleich einiger Sprachfassungen der Datenschutz-Grundverordnung hervor.

Bei insgesamt 24 Amtssprachen der EU<sup>28</sup> bleiben sprachliche Abweichungen zwischen den verschiedenen Fassungen eines Rechtsakts nicht aus und stellen daher eine allgemeine Herausforderung bei der Auslegung europäischer Rechtsakte dar.<sup>29</sup> Für die Auslegung des EU-Rechts sind, trotz der Gefahr damit be-

---

<sup>27</sup> Siehe hierzu bereits oben: Kap. 4, A. *Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.*

<sup>28</sup> Bulgarisch, Dänisch, Deutsch, Englisch, Estnisch, Finnisch, Französisch, Griechisch, Irisch, Italienisch, Kroatisch, Lettisch, Litauisch, Maltesisch, Niederländisch, Polnisch, Portugiesisch, Rumänisch, Schwedisch, Slowakisch, Slowenisch, Spanisch, Tschechisch und Ungarisch, siehe Art. 1 der Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Wirtschaftsgemeinschaft, zuletzt geändert durch die Verordnung (EU) 517/2013 des Rates vom 13. Mai 2013 zur Anpassung einiger Verordnungen und Beschlüsse in den Bereichen freier Warenverkehr, Freizügigkeit, Gesellschaftsrecht, Wettbewerbspolitik, Landwirtschaft, Lebensmittelsicherheit, Tier und Pflanzengesundheit, Verkehrspolitik, Energie, Steuern, Statistik, transeuropäische Netze, Justiz und Grundrechte, Recht, Freiheit und Sicherheit, Umwelt, Zollunion, Außenbeziehungen, Außen-, Sicherheits- und Verteidigungspolitik und Organe aufgrund des Beitritts der Republik Kroatien. Auch wenn nach dem Brexit kein EU-Mitgliedstaat Englisch als (erste) Amtssprache führt, dürfte Englisch so lange als Amtssprache in der EU gelten, bis die Verordnung einstimmig vom Rat geändert wurde (vgl. zur Kompetenz auch Art. 342 AEUV). Siehe hierzu auch Europäische Union, Sprachen, unter: [https://european-union.europa.eu/principles-countries-history/languages\\_de](https://european-union.europa.eu/principles-countries-history/languages_de).

<sup>29</sup> Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 14; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 86; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 337 ff.; *Buck*, Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, 1998, S. 152 ff.; *Roth*, *RabelsZ* 75 (2011), S. 787, 799; *Höpfner/Rütbers*, *AcP* 209 (2009), S. 1, 10; *Müller*, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391 ff.; *Weiler*, *ZEuP* 2010, S. 861, 862; *Adrian*, Grundprobleme einer juristischen (gemeinschaftsrechtlichen) Methodenlehre, 2009, S. 345.

gründeter Abweichungen, alle offiziellen Sprachfassungen verbindlich und zudem gleichrangig zu beachten.<sup>30</sup> Selbst „Arbeitssprachen“, in denen die Entwürfe des Rechtsakts erarbeitet wurden und bei denen man daher annehmen könnte, dass sie den Willen des Gesetzgebers deutlicher zum Ausdruck bringen,<sup>31</sup> genießen keinen Vorrang.<sup>32</sup>

Für die Wortlautauslegung müssen daher grds. sämtliche Sprachfassungen des Rechtsakts herangezogen werden.<sup>33</sup> Einen umfassenden Vergleich sämtli-

---

<sup>30</sup> EuGH, Rs. C-283/81 (C.I.L.F.I.T.), ECLI:EU:C:1982:335 = BeckRS 1982, 108239, Rn. 18; EuGH, Rs. C-296/95 (The Queen/Commissioners of Customs and Excise, ex parte EMU Tabac u.a.), ECLI:EU:C:1998:152 = EuZW 1998, S. 503, Rn. 36; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 14; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 86; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 342; *Roth*, *RabelsZ* 75 (2011), S. 787, 799.

<sup>31</sup> *Martens*, Methodenlehre des Unionsrechts, 2013, S. 343, im Ergebnis aber für einen Vergleich aller Sprachfassungen (siehe dort insb. Fn. 246); Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 87 im Ergebnis aber ablehnend; vgl. hierzu auch *Müller*, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391, 392, der aufgrund einzelner Arbeitssprachen den gleichrangigen Charakter (faktisch) anzweifelt, diesen aber dennoch keinen Vorrang einräumt (S. 403); vgl. auch zur Arbeit mit einzelnen Arbeitssprachen im Gesetzgebungsprozess *Weiler*, ZEuP 2010, S. 861, 865.

<sup>32</sup> Vgl. Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 16, siehe auch Rn. 14; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 87; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 342 f.; *Müller*, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391, 403.

<sup>33</sup> EuGH, Rs. C-29/69 (Stauder/Stadt Ulm), ECLI:EU:C:1969:57 = BeckRS 2004, 72956, Rn. 3; EuGH, Rs. C-268/99 (Jany u.a.), ECLI:EU:C:2001:616 = NVwZ 2002, S. 326, Rn. 47; EuGH, Rs. C-569/08 (Internetportal und Marketing), ECLI:EU:C:2010:311 = MMR 2010, S. 538, Rn. 35; EuGH, Rs. C-488/11 (Asbeek Brusse und de Man Garabito), ECLI:EU:C:2013:341 = NJW 2013, S. 2579, Rn. 26; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 14; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 342 f.; *Roth*, *RabelsZ* 75 (2011), S. 787, 799; *Müller*, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391, 403; *Weiler*, ZEuP 2010, S. 861, 866, fordert allerdings eine Befreiung der nationalen Gerichte vom Vergleich aller Sprachfassungen (S. 876 ff).

cher Sprachfassungen nimmt aber selbst der EuGH nicht vor, sondern beschränkt sich meist auf eine Auswahl von fünf bis sieben<sup>34</sup> Sprachfassungen.<sup>35</sup> Die Berücksichtigung weiterer Sprachfassungen könnte hingegen indirekt erfolgen, indem den Mitgliedstaaten die Möglichkeit gegeben wird, zu einer, beim EuGH anhängigen Rechtssache Stellung zu beziehen, bei denen die Mitgliedstaaten wohl ihre eigene Sprachfassung zugrunde legen und so mögliche Sprachdivergenzen identifiziert und durch den EuGH berücksichtigt werden könnten.<sup>36</sup>

Im Kontext des Art. 32 DS-GVO überschreibt die englische Fassung diesen mit „*Security of processing*“. Auch andere Sprachfassungen verwenden hier – wie im Deutschen – einen Begriff, der sich wohl am besten mit „*Sicherheit*“ übersetzen lässt.<sup>37</sup> In Art. 32 Abs. 1 DS-GVO wird anstelle des „*Schutzniveaus*“ allerdings eine, mit der Überschrift vergleichbare, Formulierung gewählt (bspw. im Englischen: „*level of security*“)<sup>38</sup>. Gleichzeitig stellen zudem alle untersuchten Sprachfassungen in Art. 5 Abs. 1 lit. f) DS-GVO ebenfalls auf den Begriff der

---

<sup>34</sup> Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 87. Siehe auch Müller, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391, 403 f. der den Fokus bei der Auswahl auf den Arbeitssprachen, größeren Amtssprachen und älteren Sprachfassungen sieht. Kritisch Martens, Methodenlehre des Unionsrechts, 2013, S. 341, dem allgemein die Auswahl der untersuchten Sprachen „*willkürlich anmute[t]*“.

<sup>35</sup> Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 87; kritisch Martens, Methodenlehre des Unionsrechts, 2013, S. 342 f., der wohl allenfalls in den Entscheidungsbegründungen einen Fokus auf ausgewählte Sprachen zulässt, „*gerichtsintern*“ aber stets einen Vergleich mit allen Sprachen fordert (siehe auch dort Fn. 246); Höpfner/Rüthers, AcP 209 (2009), S. 1, 10, verweisen hingegen darauf, dass eine Auslegung sämtlicher Sprachfassungen den EuGH kapazitätsbedingt überfordern könnte; auch Gebauer/Teichmann/Baldus/Raff, Europäisches Privat- und Unternehmensrecht, 2. Aufl. 2022, § 3, Rn. 96 ff.; ähnlich auch Müller, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391, 403, der den begrenzten Sprachvergleich durch den EuGH mit der steigenden Zahl der Amtssprachen begründet.

<sup>36</sup> Riesenhuber/Riesenhuber, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 14.

<sup>37</sup> Französisch: „*Sécurité du traitement*“, Spanisch: „*Seguridad del tratamiento*“, Italienisch: „*Sicurezza del trattamento*“, Niederländisch: „*Beveiliging van de verwerking*“.

<sup>38</sup> Französisch: „*niveau de sécurité*“, Spanisch: „*nivel de seguridad*“, Italienisch: „*livello di sicurezza*“, Niederländisch: „*beveiligingsniveau*“.

„angemessenen Sicherheit“ ab, wie es bspw. die englische Fassung mit „*appropriate security*“<sup>39</sup> zum Ausdruck bringt.

Anhand des Vergleichs mit den anderen Sprachfassungen – aber auch aufgrund der Überschrift des Art. 32 DS-GVO und der systematischen<sup>40</sup> Verbindung zu Art. 5 Abs. 1 lit. f) DS-GVO –<sup>41</sup> zeigt sich jedenfalls für Art. 32 DS-GVO, dass die deutsche Sprachfassung mit der Anknüpfung an den Begriff des „*Schutzniveaus*“ wohl eine terminologische Ungenauigkeit enthält.<sup>42</sup> Zum Zwecke der Normklarheit und zur Vermeidung abweichender Interpretationen wäre es daher besser gewesen, wenn die deutsche Sprachfassung in Art. 32

<sup>39</sup> Französisch „*sécurité appropriée*“, Spanisch: „*seguridad adecuada*“, Italienisch: „*un'adeguata sicurezza*“, Niederländisch: „*passende beveiliging*“.

<sup>40</sup> Siehe allgemein zur systematischen Auslegung im Europäischen Recht: EuGH, Rs. C-6/64 (Costa/E.N.E.L.), ECLI:EU:C:1964:66 = BeckRS 1964, 105086, Rn. 62, 67; EuGH, Rs. C-533/07 (Falco Privatstiftung und Rabitsch), ECLI:EU:C:2009:257 = NJW 2009, S. 1865, Rn. 33 ff.; EuGH, verb. Rs. C-402/07, C-432/07 (Sturgeon u.a.), ECLI:EU:C:2009:716 = NJW 2010, S. 43, Rn. 29 ff.; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 21 ff.; Müller/*Christensen*, Juristische Methodik, II. Bd. Europarecht, 3. Aufl. 2012, Rn. 347 ff.; Jung/*Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 95 ff.; Martens, Methodenlehre des Unionsrechts, 2013, S. 406 ff.; Buck, Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, 1998, S. 177 ff.; Henninger, Europäisches Privatrecht und Methode, 2009, S. 282 ff.; Anweiler, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 172 ff.; Höpfner/*Rütbers*, AcP 209 (2009), S. 1, 11 f.

<sup>41</sup> Sprachdivergenzen dürfen nicht ausschließlich anhand eines Sprachvergleichs (bspw. i.S.e. Mehrheitsentscheid) gelöst werden, sondern bedürfen weiterer Erkenntnisse aus anderen Auslegungsmethoden: EuGH, Rs. C-30/77 (Regina/Bouchereau), ECLI:EU:C:1977:172 = BeckRS 2004, 73063, Rn. 13/14; EuGH, Rs. C-449/93 (Rockfon/Specialarbejderforbundet i Danmark, agissant pour Søren Nielsen u.a.), ECLI:EU:C:1995:420 = NZA 1996, S. 471, Rn. 28; EuGH, Rs. C-72/95 (Kraaijeveld u.a.), ECLI:EU:C:1996:404 = NVwZ 1997, S. 473, Rn. 28; immer mit Verweis auf die Systematik und den Zweck; siehe auch aus der Literatur: Martens, Methodenlehre des Unionsrechts, 2013, S. 339; Buck, Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, 1998, S. 155 ff.; Höpfner/*Rütbers*, AcP 209 (2009), S. 1, 10; Jung/*Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 87; Müller, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391, 404; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 15; Hager, Rechtsmethoden in Europa, 2009, 6. Kap., Rn. 6; Weiler, ZEuP 2010, S. 861, 873.

<sup>42</sup> Ähnlich mit dem Verweis auf die englische Sprachfassung auch DatKomm/*Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 3; zurückhaltender Simitis/*Hornung/Spiecker* gen. Döhmman/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 30.

Abs. 1 DS-GVO ebenfalls von der „angemessenen Sicherheit“, wie in Art. 5 Abs. 1 lit. f) DS-GVO oder von einem „angemessenen Sicherheitsniveau“ gesprochen hätte.<sup>43</sup> Trotz dieser Kritik wird fortan der deutsche Begriff des Schutzniveaus beibehalten, um hier den Gleichlauf mit dem bestehenden Wortlaut der deutschen Sprachfassung zu wahren und mögliche Missverständnisse durch einen (neuen) Begriff zu vermeiden. Denn im Ergebnis hat diese Verwendung unterschiedlicher Begriffe keinen Einfluss auf die Auslegung des Art. 32 Abs. 1 DS-GVO.

## II. Risiko für die Rechte und Freiheiten (natürlicher) Personen

Neben dieser etwas ungenauen Bezeichnung in der deutschen Fassung zeigt sich in Bezug auf das angemessene Schutzniveau noch ein weiteres Problem, das dem Rechtsanwender das Verständnis über den Regelungsinhalt der Norm erschweren könnte. Art. 32 Abs. 1 DS-GVO verlangt die Gewährleistung eines „dem Risiko angemessenen Schutzniveaus“<sup>44</sup>. Was die Datenschutz-Grundverordnung unter einem angemessenen Schutzniveau nach Art. 32 Abs. 1 DS-GVO verstehen möchte, richtet sich damit wohl nach diesem Risiko. Unklar bleibt jedoch zunächst, um welches Risiko es sich hierbei handeln soll.

Der Grund dafür liegt darin, dass die Verordnung dieses Risiko im Zusammenhang mit dem angemessenen Schutzniveau nicht nennt. Mit der Verwendung des bestimmten Artikels „dem Risiko“<sup>45</sup> setzt sie das Risiko vielmehr als bekannt voraus. Diese sprachliche Technik funktioniert nur, wenn das in Frage stehende Risiko zuvor bereits benannt wurde. Mit Blick auf Art. 32 Abs. 1 DS-

<sup>43</sup> Vgl. Feiler/Forgó, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 32 DS-GVO, Rn. 7, die insofern die englischen Begriffe hervorheben.

<sup>44</sup> Englisch: „a level of security appropriate to the risk“, Französisch: „un niveau de sécurité adapté au risque“, Spanisch: „un nivel de seguridad adecuado al riesgo“, Italienisch: „un livello di sicurezza adeguato al rischio“, Niederländisch: „het risico afgestemd beveiligingsniveau“.

<sup>45</sup> Englisch: „the risk“, Französisch: „au risque“, Spanisch: „al riesgo“, Italienisch: „al rischio“, Niederländisch: „het risico“.

GVO kann sich der Verweis damit nur auf das „*Risiko für die Rechte und Freiheiten natürlicher Personen*“<sup>46</sup> beziehen, dass die Verordnung zu Beginn des Art. 32 Abs. 1 DS-GVO in einem anderen Zusammenhang<sup>47</sup> erwähnt.<sup>48</sup>

Das „*dem Risiko angemessenen Schutzniveau*“ nach Art. 32 Abs. 1 DS-GVO muss daher i.S.e. „*dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessene Schutzniveau*“ gelesen werden.<sup>49</sup>

## C. Personal data breaches (und andere Sicherheitsvorfälle)

### I. Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO

Der Schutz von Art. 32 Abs. 1 DS-GVO richtet sich daher auf ein drohendes Risiko für die Rechte und Freiheiten natürlicher Personen, für das ein angemessenes Schutzniveau gewährleistet werden soll. Die damit verbundenen Ziele der Vorschriften werden hierdurch allerdings noch nicht eindeutig konturiert.

Der Grund hierfür liegt einmal darin, dass die Rechte und Freiheiten natürlicher Personen, als geschützte Rechtsgüter, sehr umfassend und abstrakt beschrieben werden. Dazu gehört, dass der Schutz der Rechte und Freiheiten natürlicher Personen Ähnlichkeiten aufweist mit den allgemeinen Zielen der Datenschutz-Grundverordnung aus Art. 1 DS-GVO. So heißt es in Art. 1

---

<sup>46</sup> Englisch: „*the risk [...] for the rights and freedoms of natural persons*“, Französisch: „*des risques [...] pour les droits et libertés des personnes physiques*“, Spanisch: „*riesgos [...] para los derechos y libertades de las personas físicas*“, Italienisch: „*del rischio [...] per i diritti e le libertà delle persone fisiche*“, Niederländisch: „*risico's voor de rechten en vrijheden van personen*“.

<sup>47</sup> Hierzu ausführlicher: Kap. 5, B., III. *Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?*.

<sup>48</sup> Siehe Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 12; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 50; Laue/Kremer/Laue, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7, Rn. 24; Schlegel, ZD 2020, S. 243, 245.

<sup>49</sup> Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 12; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3; Schlegel, ZD 2020, S. 243, 245. Siehe auch Schneider, Datenschutz, 2. Aufl. 2019, S. 263, der bei „*dem Risiko angemessenen Schutzniveau*“ knapp auf „*die Rechte der Betroffenen*“ verweist, siehe ausführlicher hinsichtlich der Einschränkung auf die betroffene Person sogleich, Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

Abs. 2 DS-GVO, dass die Verordnung „*die Grundrechte und Grundfreiheiten natürlicher Personen*“<sup>50</sup> schützt, worunter beispielsweise<sup>51</sup> deren Recht auf Schutz personenbezogener Daten aus Art. 8 Grundrechte-Charta (GrCh) gehört. Anders jedoch als der Verweis auf die Grundrechte und Grundfreiheiten in Art. 1 Abs. 2 DS-GVO zur Beschreibung der allgemeinen Ziele der gesamten Datenschutz-Grundverordnung, könnten – jedenfalls rein vom Wortlaut betrachtet – die Rechtsgüter in Art. 32 Abs. 1 DS-GVO hier noch einmal deutlich darüber hinausgehen. Denn Art. 32 Abs. 1 DS-GVO beschränkt sich nicht auf die *Grundrechte* und *Grundfreiheiten*, sondern könnte auch einfach-gesetzlich geschützte Rechtspositionen umfassen.<sup>52</sup>

Unabhängig von einer damit denkbaren Ausweitung des Art. 32 Abs. 1 DS-GVO im Vergleich zum allgemeinen Ziel der Datenschutz-Grundverordnung nach Art. 1 Abs. 2 DS-GVO, dürfte bereits der pauschale Schutz solcher (Grund-)Rechte und (Grund-)Freiheiten selbst bei engster Auslegung der Begriffe wohl kaum geeignet sein, die Ziele einer einzelnen Rechtsvorschrift zu konkretisieren. Zwar kann die Datenschutz-Grundverordnung den Schutz der (Grund-)Rechte und (Grund-)Freiheiten als allgemeines Ziel vorgeben, um dem

---

<sup>50</sup> Englisch: „*fundamental rights and freedoms of natural persons*“, Französisch: „*les libertés et droits fondamentaux des personnes physiques*“, Spanisch: „*los derechos y libertades fundamentales de las personas físicas*“, Italienisch: „*i diritti e le libertà fondamentali delle persone fisiche*“, Niederländisch: „*de grondrechten en de fundamentele vrijheden van natuurlijke personen*“.

<sup>51</sup> Ehmann/Selmayr/Zerdick, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 1 DS-GVO, Rn. 7; Taeger/Gabel/Schmidt, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 1 DS-GVO, Rn. 13; Simitis/Hornung/Spiecker gen. Döhmman/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 1 DS-GVO, Rn 36, wonach der Schutz personenbezogener Daten (nach Art. 8 GrCh) „*herausgehoben*“ wurde; ähnlich BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 1 DS-GVO (Stand: November 2021), Rn. 5; auch Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 1 DS-GVO, Rn. 4.

<sup>52</sup> So allgemein auf den Begriff „*Risiko für die Rechte und Freiheiten natürlicher Personen*“ abstellend wohl Bieker/Bremert, ZD 2020, S. 7, 8; vgl. auch Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 24 DS-GVO, Rn. 31; jedenfalls zur wortgleichen Formulierung in Art. 24 DS-GVO; Sander, PinG 2017, S. 250, 253, hebt gerade hervor, dass „*(alle) Rechte und Freiheiten natürlicher Personen*“ erfasst sein sollen. Siehe auch Veil, ZD 2018, S. 9, 15, der im Rahmen des diesbezüglich gleichlautenden Begriffs in Art. 24 DS-GVO, allerdings mit Verweis auf die fehlende Konkretisierung des allgemeinen Schutzes der Datenschutz-Grundverordnung (und damit des Grundrechtsschutzes) einer Erfassung „*alle[r] nur denkbaren Rechte und Freiheiten natürlicher Personen*“ kritisch gegenübersteht.



Rechtsanwender eine erste Vorstellung über den Rechtsakt zu verschaffen. Die Ziele und Zwecke einzelner Regelungen der Datenschutz-Grundverordnung lassen sich hierdurch jedoch nicht konkretisieren, sondern müssen aus der konkret in Frage stehenden Vorschrift hergeleitet werden.<sup>53</sup> Es ist somit aus Art. 32 DS-GVO herzuleiten, warum und wie die Sicherheit der Verarbeitung die Rechte und Freiheiten natürlicher Personen schützen möchte.

Hilfreicher zur Bestimmung des Grunds, warum Art. 32 DS-GVO die Rechte und Freiheiten natürlicher Personen schützen möchte, wäre es gewesen, wenn die Vorschrift klargestellt hätte, wovor die Rechte und Freiheiten geschützt werden sollen, also welche Gefahren adressiert werden sollen. Aus Art. 32 Abs. 1 DS-GVO geht dies nicht hervor. Erst in Verbindung mit Art. 32 Abs. 2 DS-GVO wird klarer, worauf sich das Schutzniveau in Art. 32 Abs. 1 DS-GVO konkret beziehen könnte bzw. eher, wovor Art. 32 Abs. 1 DS-GVO eigentlich schützen möchte.<sup>54</sup>

Art. 32 Abs. 2 DS-GVO dient als Konkretisierung des angemessenen Schutzniveaus.<sup>55</sup> Dies geht bereits unmittelbar aus dem Wortlaut hervor. So heißt es

---

<sup>53</sup> Vgl. zur fehlenden Eignung „*allgemeiner Zweckrichtungen*“ bei der Auslegung: Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 42; Herresthal, ZEuP 2009, S. 598, 603 ff., am Beispiel der Verbrauchsgüterkaufrichtlinie; vgl. auch Gebauer/Teichmann/*Baldus/Raff*, Europäisches Privat- und Unternehmensrecht, 2. Aufl. 2022, § 3, Rn. 148, die „*allgemein gehaltene Zielerwägungen*“ bei der Argumentation wohl nicht berücksichtigen wollen. Siehe allgemein zu dem Problem, dass bei einem Fokus auf die (allgemeinen) Zwecke und Ziele eines Rechtsakts schutzwürdige Gegeninteressen oftmals nicht ausreichend berücksichtigt werden: *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, S. 461 ff., mit Verweis auf *Schoch*, JZ 1995, S. 109, 117 f., der von einer („strukturellen“) „*Ein-dimensionalität*“ spricht, bei der das Gemeinschaftsinteresse im Mittelpunkt steht; *Junker*, NZA 1999, S. 2, 10; Riesenhuber/*Rebbahn/Franzen*, Europäische Methodenlehre, 4. Aufl. 2021, § 17, Rn. 20. Siehe auch *Wank*, Juristische Methodenlehre, 2020, § 18, Rn. 96 ff., der kritisiert, dass der EuGH bei der „*Herausarbeitung der Ziele*“ nicht ausreichend differenziert und oftmals keine entgegenstehenden Ziele anspricht.

<sup>54</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58; *Wennemann*, DuD 2018, S. 174, 176, bezeichnet die, in Art. 32 Abs. 2 DS-GVO aufgeführten Punkte als „*Gefährdungen*“.

<sup>55</sup> Plath/*Grages*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 11; Kühling/*Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58. Siehe auch EuGH, Rs. C-340/21 (Natsionalna agentsia za prihodite), ECLI:EU:C:2023:986 = BeckRS 2023, 35786, Rn. 41.

gleich zu Beginn des Absatzes: „Bei der Beurteilung des angemessenen Schutzniveaus sind [...] zu berücksichtigen [...]“<sup>56</sup>. Problematisch ist hingegen die Umsetzung. So sind nach Art. 32 Abs. 2 DS-GVO bei der Bestimmung des angemessenen Schutzniveaus „[...] insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind [...]“<sup>57</sup>. Welche „Risiken“ dies sind, wird anschließend im Rahmen einer nicht abschließenden Aufzählung benannt.<sup>58</sup> Darunter fallen „[...] – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von, beziehungsweise unbefugten Zugang zu personenbezogenen Daten“<sup>59</sup>.

Auslegungsprobleme bereitet hier vor allem die Verwendung des Begriffs „Risiko“<sup>60</sup> in Art. 32 Abs. 1 DS-GVO bzw. „Risiken“<sup>61</sup> in Art. 32 Abs. 2 DS-GVO. Hierdurch könnte der Eindruck entstehen, dass das Risiko für die Rechte

---

<sup>56</sup> Englisch: „In assessing the appropriate level of security account shall be taken [...]“, Französisch: „Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte [...]“, Spanisch: „Al evaluar la adecuación del nivel de seguridad se tendrán [...]“, Italienisch: „Nel valutare l'adeguato livello di sicurezza, si tiene conto [...]“, Niederländisch: „Bij de beoordeling van het passende beveiligingsniveau [...] rekening gehouden [...]“.

<sup>57</sup> Englisch: „[...] in particular of the risks that are presented by processing [...]“, Französisch: „[...] en particulier des risques que présente le traitement [...]“, Spanisch: „[...] particularmente en cuenta los riesgos que presente el tratamiento de datos [...]“, Italienisch: „[...] in special modo dei rischi presentati dal trattamento [...]“, Niederländisch: „[...] wordt met name rekening gehouden met de verwerkingsrisico's [...]“.

<sup>58</sup> Hierzu sogleich noch ausführlicher unter: Kap. 4, C., II. Die Bedeutung des Begriffs „personal data breach“.

<sup>59</sup> Englisch: „[...] accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed“, Französisch: „[...] la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite“, Spanisch: „[...] la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos“, Italienisch: „[...] dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati“, Niederländisch: „[...] de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig“.

<sup>60</sup> Englisch: „risk“, Französisch: „risques“, Spanisch: „riesgos“, Italienisch: „rischio“, Niederländisch: „risico's“.

<sup>61</sup> Englisch: „risks“, Französisch: „risques“, Spanisch: „riesgos“, Italienisch: „rischi“, Niederländisch: „verwerkingsrisico's“.

und Freiheiten natürlicher Personen nach Art. 32 Abs. 1 DS-GVO ergänzt wird durch die „Risiken“ nach Art. 32 Abs. 2 DS-GVO.<sup>62</sup> Es handelt sich hierbei aber nicht um „Risiken“, die es nebeneinander zu beachten gilt. Man könnte hier allenfalls von einer „Art“ Konkretisierung des Risikos für die Rechte und Freiheiten natürlicher Personen durch die „Risiken“ nach Art. 32 Abs. 2 DS-GVO sprechen.<sup>63</sup> Allerdings dürfte hier der Begriff „Risiken“ in Art. 32 Abs. 2 DS-GVO – zumindest im Kontext des zuvor beschriebenen Risikos für die Rechte und Freiheiten natürlicher Personen – missverständlich sein.

Um dies zu verdeutlichen, muss zunächst auf den „Risikobegriff“ der Datenschutz-Grundverordnung eingegangen werden. Was die Datenschutz-Grundverordnung unter einem Risiko versteht, wird nicht ausdrücklich definiert.<sup>64</sup> Nach einem verbreiteten Verständnis setzt sich ein Risiko aus der Eintrittswahrscheinlichkeit eines (negativen) Ereignisses und der Schwere der daraus drohenden Folgen zusammen.<sup>65</sup> Auch die Datenschutz-Grundverordnung scheint

---

<sup>62</sup> Wohl in diese Richtung argumentierend Forgó/Helfrich/Schneider/Schmitz/v. Dall’Armi, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 1, Rn. 55.

<sup>63</sup> So wohl Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58, wobei sie darauf hinweist, dass andere Risiken für die Rechte und Freiheiten dennoch nicht vernachlässigt werden dürfen; Kuner/Bygrave/Docksey/Burton, GDPR, 2020, p. 636; vgl. auch Wennemann, DuD 2018, S. 174, 176, mit seiner Einteilung des Art. 32 Abs. 2 DS-GVO als „Gefährdungen“ und damit praktisch auch verbundenen mit einer Abgrenzung.

<sup>64</sup> Vgl. Bieker/Bremert, ZD 2020, S. 7, 8, jedenfalls insgesamt zum „Risiko für Rechte und Freiheiten natürlicher Personen“; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 35 DS-GVO, Rn. 15a, zu Art. 35 DS-GVO, aber wohl allgemein für die Datenschutz-Grundverordnung und anschließend auch mit einem Verweis auf Art. 32 DS-GVO (Rn. 15b); Taeger/Gabel/Lang, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 24 DS-GVO, Rn. 34, zu Art. 24 DS-GVO aber wohl ebenfalls allgemein für die Datenschutz-Grundverordnung; siehe auch allgemein zur fehlenden Definition in der Datenschutz-Grundverordnung: Schröder, ZD 2019, S. 503, 504; Ritter/Reibach/Lee, ZD 2019, S. 531, 531; Seufert, ZD 2023, S. 256, 257; Alt, DS 2020, S. 169, 169.

<sup>65</sup> Vgl. zu diesem Risikoverständnis (in verschiedenen Bereichen): Staatslexikon/Renn, 4. Bd., 8. Aufl. 2020, S. 1457, Begriff: „Risiko“; Sosnitzka/Meisterernst/Rathke, Lebensmittelrecht, Stand: 186. EL. 2023, C, Teil 1, 101. Verordnung (EG) Nr. 178/2002, Art. 3 EG-Lebensmittel-Basisverordnung, Rn. 52 ff. (Stand: November 2019); Landmann/Rohmer/Hünnekens, Umweltrecht, Bd. I, Stand: 102. EL. 2023, Umweltrecht Besonderer Teil, 1. WHG, § 73 WHG, Rn. 6 (Stand: September 2019); Müller, Hdb. Unternehmenssicherheit, 4. Aufl. 2022, S. 175; Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 74;

u.a.<sup>66</sup> in Art. 32 Abs. 1 DS-GVO diesem Verständnis zu folgen, denn sie spricht von „*der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos*“<sup>67</sup>.<sup>68</sup> Sprachlich verlagert sie aber die Faktoren der Eintrittswahrscheinlichkeiten und Schwere (der Folgen) allerdings auf die Ebene des Risikos selbst (vgl. Art. 32 Abs. 1 DS-GVO, „*unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für [...]*“<sup>69</sup>). Beide Faktoren sollten aber eher Teil des Risikobegriffs sein, aus denen dann das Risiko zu ermitteln ist.<sup>70</sup>

Genau an dieser Stelle ist anzusetzen, wenn man verstehen möchte in welchem Zusammenhang (ein Teil)<sup>71</sup> des Art. 32 Abs. 2 DS-GVO zu den Bestimmungen des Art. 32 Abs. 1 DS-GVO steht. Wie bereits angedeutet, handelt es sich bei den, in Art. 32 Abs. 2 DS-GVO aufgeführten „Risiken“ nicht um Risi-

---

Rippe, ZphF 67 (2013), S. 517, 517; vgl. Kremer u.a./Bachmann, DCGK, 9. Aufl. 2023, Teil 3, Grundsatz 4, Rn. 27; MüKo HGB/Jickeli, 5. Aufl. 2022, § 116 HGB, Rn. 13.

<sup>66</sup> Vgl. ähnlich auch Art. 24, 25 DS-GVO.

<sup>67</sup> Englisch: „*the risk of varying likelihood and severity*“, Französisch: „*des risques, dont le degré de probabilité et de gravité varie*“, Spanisch: „*riesgos de probabilidad y gravedad variables*“, Italienisch: „*del rischio di varia probabilità e gravità*“, Niederländisch: „*de qua waarschijnlijkheid en ernst uiteenlopende risico's*“.

<sup>68</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 28; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 13; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 23; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 50; Ritter/Reibach/Lee, ZD 2019, S. 531, 531; Seufert, ZD 2023, S. 256, 257; Bieker/Bremert, ZD 2020, S. 7, 8; Johannes/Geminn, InTeR 2021, S. 140, 141; Schröder, ZD 2019, S. 503, 504; Jungkind/Koch, ZD 2022, S. 656, 659; Bieker/Bremert/Hansen, DuD 2018, S. 492, 493. Stellenweise wird auch auf das Kurzpapier Nr. 18 der Datenschutzkonferenz der deutschen Datenschutzbehörden des Bundes und der Länder (DSK) verwiesen (DSK, Kurzpapier Nr. 18, S. 1).

<sup>69</sup> Englisch „*the risk of varying likelihood and severity for [...]*“, Französisch: „*des risques, dont le degré de probabilité et de gravité varie, pour [...]*“, Spanisch: „*riesgos de probabilidad y gravedad variables para [...]*“, Italienisch: „*del rischio di varia probabilità e gravità per [...]*“, Niederländisch: „*de qua waarschijnlijkheid en ernst uiteenlopende risico's voor [...]*“.

<sup>70</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 13 weist auf diese missverständliche Formulierung der DS-GVO hin; wohl auch hierauf verweisend Bieker, DuD 2018, S. 27, 29.

<sup>71</sup> Dies umfasst noch nicht das gesamte Verhältnis zwischen Art. 32 Abs. 1 und Abs. 2 DS-GVO. Das weitere Zusammenspiel der beiden Absätze wird ausführlicher unter Kap. 7, C., II., 2., c) *Offene Aufzählung der (äußeren) ersten Ebene* behandelt.

ken in diesem vergleichbaren Sinne. Die Verordnung führt hier vielmehr die negativen Ereignisse auf, die anhand ihrer Eintrittswahrscheinlichkeiten und der Schwere ihrer Folgen erst das Risiko für die Rechte und Freiheiten bestimmen.<sup>72</sup> Bei diesen negativen Ereignissen, die Art. 32 Abs. 2 DS-GVO u.a. beschreibt, handelt es sich um Sicherheitsvorfälle.<sup>73</sup>

Anders als der Wortlaut des Art. 32 Abs. 1 DS-GVO dies suggeriert, liegt das vorrangige Ziel damit nicht im generellen Schutz der Rechte und Freiheiten natürlicher Personen, sondern in dem Schutz vor einem solchen Sicherheitsvorfall während der Verarbeitung personenbezogener Daten.<sup>74</sup> Treten solche Sicher-

---

<sup>72</sup> Vgl. Wennemann, DuD 2018, S. 174, 176, der von „Gefährdungen“ spricht; siehe auch die nachfolgenden Stimmen, die besonders herausstellen, dass es sich um Ereignisse handelt: Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 5, „Katalog der [...] häufigsten Ereignisse“; Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 11, „Katalog von Ereignissen“; vgl. auch Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 50 „(ungewissen) Verletzungsereignisses“ i.V.m. Rn. 52 mit Bezug auf die Aufzählung nach Art. 32 Abs. 2 DS-GVO.

<sup>73</sup> Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58; vgl. auch Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 5, „nicht ordnungsgemäßen Verarbeitung“; Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 11, „Störungen“.

<sup>74</sup> So auch Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 14, mit dem Verweis auf den Schutz vor einem personal data breach (Art. 4 Nr. 12 DS-GVO). Zur Bedeutung des Art. 4 Nr. 12 DS-GVO im Rahmen des Art. 32 DS-GVO sogleich: Kap. 4, C., II. Die Bedeutung des Begriffs „personal data breach“. A.A. wohl Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58, die die „Risiken eines Sicherheitsvorfalls“ in den Fokus stellt, aber nach ihr auch andere „Risiken“ (wohl auch innerhalb des Art. 32 DS-GVO) nicht unberücksichtigt bleiben dürfen; ähnlich Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31, die den personal data breach (nur) „im Fokus“ sieht; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 9, verweist hingegen allgemein auf ein weites Verständnis aufgrund der Erwägungsgründe; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 19, allgemein mit dem Verweis auf die „Ausführung der DSGVO“; siehe auch Johannes/Geminn, InTeR 2021, S. 140, 141, die wohl auch Risiken aus der „geplanten, zulässigen und ordnungsgemäß durchgeführten Datenverarbeitung“ berücksichtigen wollen; auch Bieker/Bremert/Hansen, DuD 2018, S. 492, 493, berücksichtigen die Risiken der geplanten Datenverarbeitung, allerdings im Fokus der allgemeinen Risikobewertung der DS-GVO und nur später (S. 494) wird kurz auf die Bedeutung dieser Bewertung u.a. für Art. 32 DS-GVO

heitsvorfälle ein, hat dies zwar richtigerweise Einfluss auf die Rechte und Freiheiten natürlicher Personen. Aber nicht jedes Risiko für die Rechte und Freiheiten natürlicher Personen entsteht durch einen Sicherheitsvorfall. In dieser Unterscheidung liegt ein weiterer Hinweis, warum das Risiko für die Rechte und Freiheiten natürlicher Personen nicht der Hauptanknüpfungspunkt von Art. 32 DS-GVO sein kann, um dessen Ziel zu konkretisieren. Denn erst durch die Definition der Gefahren eines Sicherheitsvorfalls, vor denen Art. 32 DS-GVO schützen möchte, erlangt die Vorschrift ihren datenschutzrechtlichen Bezug.

Denn nochmal: Stellt man einzig auf das Risiko für die Rechte und Freiheiten natürlicher Personen ab und soll hierfür ein angemessenes Schutzniveau schaffen, könnten davon praktisch sämtliche Auswirkungen auf die Rechtspositionen natürlicher Personen umfasst sein, ohne dass hierfür auch nur irgend ein datenschutzrechtlicher Bezug vorliegen müsste. Als Teil der Datenschutz-Grundverordnung kann Art. 32 DS-GVO aber seinen Anwendungsbereich nicht über den Regelungsgehalt der Verordnung – den Datenschutz – ausdehnen. Wie aus der Überschrift des Art. 32 DS-GVO hervorgeht, ist das aber auch nicht das Ziel der Vorschrift. Es geht eben um die Sicherheit *der Verarbeitung* personenbezogener Daten.

Wie bereits zu Beginn des Abschnitts angesprochen, setzt sich die Datenschutz-Grundverordnung insgesamt das Ziel, die (Grund-)Rechte und (Grund-)Freiheiten bei der Verarbeitung personenbezogener Daten zu schützen (vgl. Art. 1 DS-GVO). Dabei werden die Rechte und Freiheiten bereits durch die Verarbeitung personenbezogener Daten selbst beeinträchtigt.<sup>75</sup> Ob diese Beeinträchtigung hinzunehmen ist, richtet sich dabei danach, ob personenbezogene Daten überhaupt rechtskonform verarbeitet werden dürfen, also vor allem, ob eine Rechtsgrundlage i.S.d. Art. 6 ff. DS-GVO vorliegt.<sup>76</sup> Art. 32 DS-GVO hingegen baut auf den Ergebnissen der Art. 6 ff. DS-GVO auf und gilt für jede (und

---

verwiesen; ähnlich (bereits) *Bieker*, DuD 2018, S. 27, 29, der ebenfalls im Rahmen der allgemeinen Risikobewertung der DS-GVO auf die Risiken der Verarbeitung selbst abstellt.

<sup>75</sup> Siehe hierzu bereits: Kap. 2, A., II. *Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO*.

<sup>76</sup> Siehe Kap. 2, A., II. *Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO*. Siehe ausführlicher zur Frage, ob eine Datenverarbeitung auf eine Rechtsgrundlage gestützt werden kann, anhand des Untersuchungsgegenstands: Teil 3 *Die Rechtmäßigkeit datenverarbeitender TOM*.

damit gerade auch für die i.S.d. Art. 6 ff. DS-GVO rechtskonforme) Verarbeitung personenbezogener Daten.<sup>77</sup> Die Beeinträchtigung, die sich aus der geplanten Datenverarbeitungen selbst ergeben (also überhaupt verarbeitet werden) dürften daher nicht von Art. 32 DS-GVO umfasst sein.<sup>78</sup>

Art. 32 DS-GVO braucht damit einen anderen Anknüpfungspunkt, die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu schützen. Dieser Anknüpfungspunkt liegt nicht in Art. 32 Abs. 1 DS-GVO, sondern in Art. 32 Abs. 2 DS-GVO. Das Ziel von Art. 32 DS-GVO liegt daher im Schutz der Rechte und Freiheiten natürlicher Personen vor den Gefahren eines Sicherheitsvorfalls bei der Verarbeitung personenbezogener Daten.

Diese Aufgabe der Sicherheit der Verarbeitung kam innerhalb der früheren Datenschutzrichtlinie von 1995<sup>79</sup> noch wesentlich deutlicher heraus. So hieß es in Art. 17 Abs. 1 der Datenschutzrichtlinie (DS-RL), als Vorgängerregelung zu Art. 32 DS-GVO,<sup>80</sup> noch, dass: „[...] *der für die Verarbeitung Verantwortliche*

---

<sup>77</sup> Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27, wonach es erst einer Rechtsgrundlage nach Art. 6 DS-GVO bedarf; John/Schaller, CR 2022, S. 156, 156, wonach ein „effektiver Datenschutz“ sich aus der „Zulässigkeit der Datenverarbeitung“ und der „Sicherheit der Verarbeitung“ zusammensetzt; vgl. Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 1 f., „Neben dem Vorliegen eines Erlaubnistatbestands (Art. 6) [...] bedarf es auch eines Schutzes auf faktischer Ebene [...]“.

<sup>78</sup> A.A. wohl Johannes/Geminn, InTeR 2021, S. 140, 141, die diese Risiken wohl auch berücksichtigen wollen; siehe auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 59, wonach „unerwünschte Ereignisse“ im Vordergrund stehen (damit werden von ihr aber andere Risiken nicht vollständig aus dem Anwendungsbereich ausgeschlossen); ähnlich Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31. Siehe auch in Bezug auf die allgemeine Risikobewertung: Bieker/Bremert/Hansen, DuD 2018, S. 492, 493, die die Risiken der geplanten Datenverarbeitung berücksichtigen wollen (und später wird u.a. auch für die Bedeutung der Risikobewertung auf Art. 32 DS-GVO verwiesen, S. 494); ähnlich (bereits) Bieker, DuD 2018, S. 27, 29, der ebenfalls im Rahmen der allgemeinen Risikobewertung der DS-GVO auf die Risiken der „Verarbeitung selbst“ abstellt.

<sup>79</sup> 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.

<sup>80</sup> BeckOK Datenschutzrecht/Paulus, Stand: 46. Ed. 2023, Art. 32 DS-GVO (Stand: November 2021), Rn. 2; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 2; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 21; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO,

die geeigneten technischen und organisatorischen Maßnahmen durchführen muß, die für den Schutz gegen [insb. der auch in Art. 32 Abs. 2 DS-GVO genannten Sicherheitsvorfälle]<sup>81</sup> erforderlich sind.“<sup>82</sup> Warum der Gesetzgeber in Art. 32 DS-GVO von der Formulierung des Art. 17 DS-RL abgewichen ist und die Aussage nunmehr auf zwei Absätze verteilt hat, ist nicht bekannt.

## II. Die Bedeutung des Begriffs „personal data breach“

Mit Art. 32 Abs. 2 DS-GVO rückt zusätzlich der Begriff der „Verletzung des Schutzes personenbezogener Daten“ gem. Art. 4 Nr. 12 DS-GVO in den Fokus des allgemeinen Regelungsinhalts und bedarf einer näheren Betrachtung. Vorab scheint auch hier die deutsche Übersetzung wieder etwas missverständlich zu sein. Denn ausgehend vom deutschen Wortlaut könnte man den Begriff auch allgemein als eine Verletzung einer datenschutzrechtlichen Vorschrift betrachten, da es schließlich das allgemeine Ziel des Datenschutzrechts ist, den Schutz personenbezogener Daten zu gewährleisten (vgl. Art. 1 Abs. 2 DS-GVO i.V.m. insb. Art. 8 GrCh) oder genauer die Person hinter diesen Daten zu schützen (vgl.

---

Rn. 4; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 1.

<sup>81</sup> Die Aufzählung der Sicherheitsvorfälle weicht von Art. 32 Abs. 2 DS-GVO im Wortlaut ab, da die Datenschutzrichtlinie wohl noch zu jedem einzelnen Punkt die Wertungen bspw. „unrechtmäßige Zerstörung“ anführt und in Art. 32 Abs. 2 DS-GVO dies vorne zusammenfasst „– ob unbeabsichtigt oder unrechtmäßig –“. Ferner enthält Art. 17 Abs. 1 DS-RL noch den Zusatz „und gegen jede andere Form der unrechtmäßigen Verarbeitung“, was wohl ein Hinweis auf eine nicht abschließende Aufzählung sein soll.

<sup>82</sup> Englisch: „[...] the controller must implement appropriate technical and organizational measures to protect personal data against [...]“, Französisch: „[...] le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre [...]“, Spanisch: „[...] responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra [...]“, Italienisch: „[...] il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla [...]“, Niederländisch: „[...] de voor de verwerking verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer dient te leggen om persoonsgegevens te beveiligen tegen [...]“.



Art. 1 Abs. 1 DS-GVO)<sup>83,84</sup> Ein so weites Verständnis ist von dem Begriff nach Art. 4 Nr. 12 DS-GVO aber ausgehend von der nachfolgenden Definition gerade nicht umfasst.<sup>85</sup> Denn danach handelt es sich konkret um eine Verletzung der Sicherheit.

Ein Sprachvergleich zeigt hier erneut, dass andere Fassungen treffendere Formulierungen für den zu definierenden Begriff verwenden. Am deutlichsten dürfte von den untersuchten Sprachfassungen die spanische Version sein. Diese definiert in Art. 4 Nr. 12 DS-GVO die „Verletzung der Sicherheit von personenbezogenen Daten“ („*violación de la seguridad de los datos personales*“) und schafft somit einen Gleichklang zwischen dem Begriff selbst und seiner Definition. Die französische und italienische Sprachfassung verweisen eher auf die „Verletzung personenbezogener Daten“ (Französisch: „*violation de données à*

---

<sup>83</sup> DatKomm/Lachmayer, Stand: 76. EL. 2023, Art. 1 DS-GVO (Stand: Februar 2019), Rn. 27; Gola/Heckmann/Pötters, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 1 DS-GVO, Rn. 8; Taeger/Gabel/Schmidt, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 1 DS-GVO, Rn. 7; Moos/Schefzig/Arning/Moos, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 2, Rn. 4; kritisch wohl Sydow/Marsch/Sydow, DS-GVO – BDSG, 3. Aufl. 2022, Art. 1 DS-GVO, Rn. 10 ff., der mit dem Schutz personenbezogener Daten auf eine Abkehr vom Schutz der Privatsphäre hinweist; Veil, NVwZ 2018, S. 686, 691 f. sieht kritisch in der DS-GVO einen, über das Persönlichkeitsrecht hinausgehenden Schutz, der allerdings nicht klar definiert wird und befürwortet eine Rückkehr zum Schutz des Persönlichkeitsrechts (S. 694).

<sup>84</sup> Auf diese Interpretationsmöglichkeit verweist wohl auch Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 919, wonach „*alle Vorgaben der DS-GVO dem Schutz personenbezogener Daten dienen*“, diese aber mit Blick auf die Definition ablehnt (Rn. 919 f.); siehe auch zu einer ähnlichen Interpretationsmöglichkeit mit Verweis auf den Wortlaut Bieker/Bremert/Hansen, DuD 2018, S. 492, 496, „*beliebiger Datenschutzverstoß*“, im Ergebnis aber ablehnend.

<sup>85</sup> Vgl. Ehmann/Selmayr/Klabunde, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 58, „*nicht sämtliche Verstöße gegen Datenschutzrecht*“ umfasst; Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 919 f.; Bieker/Bremert/Hansen, DuD 2018, S. 492, 496; Wybitul/Schreibauer/Spittka, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 33 DS-GVO, Rn. 11; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 12 DS-GVO, Rn. 3; Simitis/Hornung/Spiecker gen. Döhmann/Dix, Datenschutzrecht, 2019, Art. 4 Nr. 12 DS-GVO, Rn. 4; Taeger/Gabel/Arning/Rotbkegel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 368 ff.; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 4 DS-GVO, Rn. 177; BeckOK Datenschutzrecht/Schild, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 133; siehe auch Folkerts, ZD 2023, S. 654, 654 ff., zur Differenzierung zwischen „*Datenschutzverletzung*“ i.S.d. Art. 4 Nr. 12 DS-GVO und „*unrechtmäßige Datenverarbeitung*“.

*caractère personnel*“, Italienisch: „*violazione dei dati personali*“). Auch die niederländische Sprachfassung scheint in diese Richtung zu verstehen zu sein, indem sie auf die „Verletzungen im Zusammenhang mit personenbezogenen Daten“ („*inbreuk in verband met persoonsgegevens*“) abstellt. Im Vergleich zur französischen und italienischen Fassung dürfte die niederländische Formulierung jedoch etwas weiter gefasst sein. Die englische Sprachfassung definiert in Art. 4 Nr. 12 DS-GVO den „*personal data breach*“ und geht damit ebenfalls eher von einer „Verletzung personenbezogener Daten“ aus. Im Gegensatz zur französischen und italienischen Fassung verwendet die englische Sprachfassung einen Begriff, der fast schon als Eigenbegriff verstanden werden könnte. Um Missverständnisse zu vermeiden, ist es daher sinnvoll, fortan den englischen Begriff des „*personal data breach*“ zugrunde zu legen.

Bereits aus der Charakterisierung als „*Verletzung der Sicherheit*“<sup>86</sup> wird deutlich, dass die Definition des *personal data breach* in einem engen Zusammenhang mit der Sicherheit der Verarbeitung nach Art. 32 DS-GVO steht.<sup>87</sup> Darüber hinaus zählt Art. 4 Nr. 12 DS-GVO in der weiterführenden Definition –

---

<sup>86</sup> Englisch: „*breach of security*“, Französisch: „*violation de la sécurité*“, Spanisch: „*violación de la seguridad*“, Italienisch: „*la violazione di sicurezza*“, Niederländisch: „*inbreuk op de beveiliging*“.

<sup>87</sup> Taeger/Gabel/Arning/Rothkegel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 368; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 12 DS-GVO, Rn. 3; Folkerts, ZD 2023, S. 654, 654; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Art. 32 DS-GVO, Rn. 6; Knyrim/Zavadil, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 11.10; John/Schaller, CR 2022, S. 156, 156; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 4 DS-GVO, Rn. 177; Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58; Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 1, 14; Wýbitul, NJW 2020, S. 2577, Rn. 7 f.; Spiecker gen. Döhmann u.a./Dix, GDPR, 2023, Art. 4(12) GDPR, Rn. 1; Ehmann/Selmayr/Klabunde, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 56; Freund u.a./Strassemeyer/Quiel, DSGVO, 2023, Art. 4 DS-GVO, Rn. 270 f.

u.a. in der deutschen<sup>88</sup> Fassung fast, in der englischen<sup>89</sup> und spanischen<sup>90</sup> Fassung sogar wortgleich – die Sicherheitsvorfälle des Art. 32 Abs. 2 DS-GVO<sup>91</sup> auf.<sup>92</sup>

Weitere Hinweise auf die enge Verbindung beider Vorschriften ergeben sich zudem aus der Gesetzessystematik.<sup>93</sup> In der gesamten Verordnung verweisen nur zwei Artikel auf die Definition des personal data breach nach Art. 4 Nr. 12 DS-GVO. Hierbei handelt es sich um die Art. 33 und 34 DS-GVO, die im Falle eines personal data breach Mitteilungs- bzw. Benachrichtigungspflichten an die zu-

---

<sup>88</sup> Deutsch: „[...] ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“, Französisch: „[...] de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données“, Italienisch: „[...] che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati“, Niederländisch: „[...] per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens“.

<sup>89</sup> Englisch: „[...] accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed“. Mit dem einzigen Unterschied eines Kommas nach „access to“.

<sup>90</sup> Spanisch: „[...] e la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos“.

<sup>91</sup> Siehe hierzu bereits: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO*, insbesondere Fn. 59.

<sup>92</sup> Siehe hierzu auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, *Datenschutzrecht*, 2019, Art. 32 DS-GVO, Rn. 58; Taeger/Gabel/Arning/Rothkegel, *DSGVO – BDSG – TTDSG*, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 368; v. Lewinski/Rüpk/Eckhardt, *Datenschutzrecht*, 2. Aufl. 2022, § 19, Rn. 30; Freund u.a./Strassemeyer/Quiel, *DSGVO*, 2023, Art. 4 DS-GVO, Rn. 270; vgl. auch Kühling/Buchner/Jandt, *DS-GVO – BDSG*, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31.

<sup>93</sup> Siehe allgemein zur systematischen Auslegung im Europäischen Recht statt vieler: EuGH, Rs. C-6/64 (Costa/E.N.E.L.), ECLI:EU:C:1964:66 = BeckRS 1964, 105086, Rn. 62, 67; Riesenhuber/Riesenhuber, *Europäische Methodenlehre*, 4. Aufl. 2021, § 10, Rn. 21 ff. Siehe hierzu ausführlicher: Kap. 4, B., I. *Der Begriff des „Schutzniveaus“* und dort die Nachweise in Fn. 40.

ständige Aufsichtsbehörde (Art. 33 DS-GVO) bzw. an die betroffenen Personen (Art. 34 DS-GVO) begründen können.<sup>94</sup> Art. 33 und Art. 34 DS-GVO bilden wiederum gemeinsam mit Art. 32 DS-GVO den 2. Abschnitt im 4. Kapitel der Datenschutz-Grundverordnung<sup>95</sup>.<sup>96</sup> Dazu kommt noch, dass dieser Abschnitt nur aus diesen drei Vorschriften besteht. Dies ist ein klares Zeichen dafür, dass es sich hierbei um ein geschlossenes System innerhalb der Datenschutz-Grundverordnung handeln soll.<sup>97</sup>

---

<sup>94</sup> BeckOK Datenschutzrecht/*Schild*, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 133; Gola/Heckmann/*Gola*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 4 DS-GVO, Rn. 111; Taeger/Gabel/*Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 365; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 12 DS-GVO, Rn. 2; Paal/Pauly/*Ernst*, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 DS-GVO, Rn. 92.

<sup>95</sup> Zur Beachtung der Gliederung des Rechtsakts im Rahmen der Auslegung: EuGH, Rs. C-6/64 (Costa/E.N.E.L.), ECLI:EU:C:1964:66 = BeckRS 1964, 105086, Rn. 62, 67; EuGH, Rs. C-59/75 (Manghera u.a.), ECLI:EU:C:1976:14 = BeckRS 2004, 73375, Rn. 6/8; EuGH, Rs. C-678/18 (Procureur-Generaal bij de Hoge Raad der Nederlanden), ECLI:EU:C:2019:998 = GRUR 2020, S. 108, Rn. 35 ff.; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 23; *Henninger*, Europäisches Privatrecht und Methode, 2009, S. 283; *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 173; *Buck*, Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, 1998, S. 178; *Adrian*, Grundprobleme einer juristischen (gemeinschaftsrechtlichen) Methodenlehre, 2009, S. 451; *Müller/Christensen*, Juristische Methodik, II. Bd. Europarecht, 3. Aufl. 2012, Rn. 62.

<sup>96</sup> Auf die Systematik verweisen: *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 1; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 1a; Ehmman/Selmayr/*Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 3; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 3; Kuner/Bygrave/Docksey/*Tosoni*, GDPR, 2020, p. 191.

<sup>97</sup> Siehe auch Ehmman/Selmayr/*Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 3, wonach es sich bei Art. 32 DS-GVO um die „Grundlagennorm“ für Art. 33, 34 DS-GVO handelt; Paal/Pauly/*Ernst*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 12; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 3; Kuner/Bygrave/Docksey/*Burton*, GDPR, 2020, p. 632; *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 1; *Becker*, ZD 2020, S. 175, 176 f.; *John/Schaller*, CR 2022, S. 156, 156; Gierschmann u.a./*Gierschmann*, Datenschutz-Grundverordnung, 2018, Art. 33 DS-GVO, Rn. 5; vgl. auch Hornung/Schallbruch/*Jandt*, IT-Sicherheitsrecht, 2021, § 17, Rn. 30.

Legt man diesen Systemgedanken zugrunde, dann gestaltet sich das Verhältnis der Vorschriften zueinander wie folgt: Art. 32 DS-GVO legt die Anforderungen an die Sicherheit der Verarbeitung fest, um den Eintritt eines personal data breach zu verhindern oder die Folgen abzumildern.<sup>98</sup> Kommt es zu einem personal data breach, kann dies die Mitteilungs- und Benachrichtigungspflichten nach Art. 33, 34 DS-GVO auslösen. Ergänzend ist dann zu fragen, ob eine unzureichende Sicherheit und damit ein Verstoß gegen Art. 32 DS-GVO die Ursache für den personal data breach war.<sup>99</sup>

### III. Anwendung auf (andere) Sicherheitsvorfälle

Bei näherer Betrachtung könnte ein wesentlicher Aspekt diesem naheliegenden System jedoch entgegenstehen. Zunächst fällt auf, dass Art. 32 Abs. 2 DS-GVO – anders als die Art. 33, 34 DS-GVO – gerade nicht auf den Begriff des personal data breach aus Art. 4 Nr. 12 DS-GVO verweist. Art. 32 Abs. 2 DS-GVO zieht es vor, den wesentlichen Teil der Definition (fast) vollständig<sup>100</sup> zu wiederholen. Abgesehen von der sprachlichen Abweichung einzelner Fassungen der Datenschutz-Grundverordnung zeigt sich im direkten Vergleich zwischen Art. 32 Abs. 2 und Art. 4 Nr. 12 DS-GVO jedoch noch ein feiner, aber deutlicher Unterschied, der dies erklären könnte. In Art. 32 Abs. 2 DS-GVO werden die „Risiken, die mit der Verarbeitung verbunden sind“ (bzw. die Sicherheitsvorfälle)

---

<sup>98</sup> Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 1, 14; John/Schaller, CR 2022, S. 156, 156; wohl auch Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 3, mit der Einordnung als „Grundlagennorm“; vgl. auch Gierschmann u.a./Gierschmann, Datenschutz-Grundverordnung, 2018, Art. 33 DS-GVO, Rn. 5.

<sup>99</sup> Nicht jeder personal data breach muss zwingend auf einen Verstoß gegen Art. 32 DS-GVO zurückzuführen sein: Becker, ZD 2020, S. 175, 177; v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 1, Fn. 1; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 12 DS-GVO, Rn. 6; vgl. auch Simitis/Hornung/Spiecker gen. Döhmman/Dix, Datenschutzrecht, 2019, Art. 4 Nr. 12 DS-GVO, Rn. 4, verweist jedoch anstelle des Art. 32 DS-GVO auf den verwandten Datenschutzgrundsatz des Art. 5 Abs. 1 lit. f) DS-GVO; siehe ebenfalls Kuner/Bygrave/Docksey/Burton, GDPR, 2020, p. 632, dass ein Verstoß gegen Art. 32 DS-GVO sich oftmals durch einen personal data breach zeigt.

<sup>100</sup> Siehe hierzu zuvor: Kap. 4, C., II. Die Bedeutung des Begriffs „personal data breach“.

mit einem „*insbesondere*“<sup>101</sup> aufgezählt, was auf eine nicht abschließende Aufzählung hinweist.<sup>102</sup> Die Definition in Art. 4 Nr. 12 DS-GVO ist hingegen abschließend formuliert.<sup>103</sup> Inhaltlich könnte dies zur Folge haben, dass ein personal data breach zwar eine Verletzung der Sicherheit darstellt, dieser aber nur einen wichtigen Unterfall ausmacht und die Sicherheit der Verarbeitung nach Art. 32 DS-GVO damit weiter gefasst ist.<sup>104</sup>

Daran knüpfen insbesondere zwei Folgefragen an. Stellt der personal data breach nur einen wichtigen Unterfall der Sicherheit der Verarbeitung dar, so müsste geklärt werden, welche anderen Sicherheitsvorfälle von Art. 32 Abs. 2 DS-GVO umfasst sind, die es zu berücksichtigen gilt, aber deren Verletzung keinen personal data breach i.S.d. Art. 4 Nr. 12 DS-GVO darstellen. Hinweise in der Verordnung selbst finden sich hierzu nicht. Unklar bleibt zweitens auch, warum eine Verletzung dieser (anderen) Sicherheitsvorfälle gerade keine Melde- und Benachrichtigungspflichten i.S.d. Art. 33, 34 DS-GVO nach sich ziehen sollten. Der Wortlaut scheint dem Systemgedanken hier entgegenzustehen.

Aus systematischen und auch teleologischen Erwägungen erscheint ein in sich geschlossener Regelungsabschnitt und damit ein Gleichklang zwischen Art. 32 Abs. 2 DS-GVO und Art. 4 Nr. 12 DS-GVO vorzugswürdiger. Überlegenswert wäre daher, ob man im Rahmen einer – in der europäischen Methodik nicht so bezeichneten aber dem Wesen nach anerkannten –<sup>105</sup> teleologischen

<sup>101</sup> Englisch: „*in particular*“, Französisch: „*notamment*“, Spanisch: „*en particular*“, Italienisch: „*in particolare*“, Niederländisch: „*vooral*“.

<sup>102</sup> VG Mainz, CR 2021, S. 471, Rn. 37; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 40; Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10; Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 23; Wennemann, DuD 2018, S. 174, 176.

<sup>103</sup> Simitis/Hornung/Spiecker gen. Döhmman/*Dix*, Datenschutzrecht, 2019, Art. 4 Nr. 12 DS-GVO, Rn. 7; Taeger/Gabel/*Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 373.

<sup>104</sup> Dahingehend wohl Simitis/Hornung/Spiecker gen. Döhmman/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58, wonach darin (nur) der Fokus liegt; auch Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31.

<sup>105</sup> Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 174; vgl. Riesenhuber/*Neuner*, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 38; siehe aber die Verwendung des Begriffs in einigen Schlussanträgen der Generalanwältin: *GA Medina*, Schlussanträge v. 29.06.2023 zur verb. Rs. C-207/22, C-267/22, C-290/22 (*Lineas – Concessões de Transportes*), ECLI:EU:C:2023:533, Rn. 72; *GA Kokott*,

Reduktion<sup>106</sup> das „insbesondere“ in der Aufzählung des Art. 32 Abs. 2 DS-GVO „streicht“ und damit auf die genannten Sicherheitsvorfälle reduziert und so faktisch mit Art. 4 Nr. 12 DS-GVO gleichsetzt. Alternativ könnte man auch einen personal data breach und damit die anknüpfenden Melde- und Benachrichtigungspflichten analog<sup>107</sup> auf Sicherheitsvorfälle anwenden, die zwar unter Art. 32 Abs. 2 DS-GVO aber nicht unter den jetzigen Art. 4 Nr. 12 DS-GVO fallen.

Ob ein rechtsfortbildender Eingriff (faktisch) jedoch notwendig ist, bleibt noch zu klären. So ist zu bedenken, dass die erfassten Sicherheitsvorfälle in Fall-

---

Schlussanträge v. 01.03.2018 zur verb. Rs. C-118/16, C-115/16, C-118/16, C-119/16, C-299/16 (X Denmark), ECLI:EU:C:2018:146, Rn. 94; *GA Bobek*, Schlussanträge v. 22.06.2016 zur Rs. C-177/15 (Nelsons), ECLI:EU:C:2016:474, Rn. 37; *GA Trstenjak*, Schlussanträge v. 14.05.2009 zur Rs. C-199/08 (Eschig), ECLI:EU:C:2009:310, Rn. 80, 82.

<sup>106</sup> Allgemein zum Instrument der „teleologischen Reduktion“ in der europäischen Methodik: *Riesenhuber/Neuner*, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 38 ff.; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 174 f.; *Henninger*, Europäisches Privatrecht und Methode, 2009, S. 392 f.; *Müller/Christensen*, Juristische Methodik, II. Bd. Europarecht, 3. Aufl. 2012, Rn. 84. Siehe auch einige Urteile des EuGH, in denen nach Auffassung der Literatur das Gericht nach deutschem Verständnis eine „teleologische Reduktion“ anwendet: EuGH, Rs. C-81/79 (Sorasio-Allo u.a./Kommission), ECLI:EU:C:1980:270 = BeckRS 2004, 73763, Rn. 15; EuGH, Rs. C-183/90 (Van Dalfsen u.a./Van Loon u.a.), ECLI:EU:C:1991:379 = BeckRS 2004, 74756, Rn. 19 ff.; EuGH, Rs. C-41/15 (Dowling u.a.), ECLI:EU:C:2016:836 = EuZW 2016, S. 955, Rn. 49 ff.

<sup>107</sup> Allgemein zur Anerkennung der „Analogie“ in der europäischen Methodik: *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 305 ff.; *Riesenhuber/Neuner*, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 33 f.; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 167 ff.; *Schön*, Die Analogie im Europäischen (Privat-)Recht, in: FS Canaris zum 80. Geburtstag, 2017, S. 147 ff.; *Langenbucher/Langenbucher/Donath*, Europäisches Privat- und Wirtschaftsrecht, 5. Aufl. 2022, § 1, Rn. 22; *Gebauer/Teichmann/Baldus/Raff*, Europäisches Privat- und Unternehmensrecht, 2. Aufl. 2022, § 3, Rn. 211 ff., sprechen der Analogie im Unionsrecht nur eine geringe Bedeutung zu. Siehe auch einige Urteile des EuGH, in denen nach Auffassung der Literatur das Gericht nach deutschem Verständnis eine „Analogie“ anwendet: EuGH, Rs. C-180/78 (Brouwer-Kaune), ECLI:EU:C:1979:156 = BeckRS 2004, 72048, Rn. 7 f.; EuGH, Rs. C-165/84 (Krohn/BALM), ECLI:EU:C:1985:507 = BeckRS 2004, 71892, Rn. 23 ff.; EuGH, Urteil v. 19.11.2009, verb. Rs. C-402/07, C-432/07 (Sturgeon u.a.), ECLI:EU:C:2009:716 = NJW 2010, S. 43, Rn. 40 ff.

gruppen dargestellt werden. Einige der, beiden Vorschriften übereinstimmenden, Fallgruppen eines Sicherheitsvorfalls können dabei sehr weit interpretiert werden. Ob damit noch ein großer Raum für weitere, nicht benannte und dann nicht unter Art. 4 Nr. 12 DS-GVO fallende Sicherheitsvorfälle bleibt, ist zu bezweifeln. Eine Entscheidung in dieser Frage und einer möglichen Lösung mittels einer Rechtsfortbildung bedarf es – ohne nähere Untersuchung – für die weitere Bearbeitung nicht. Da der Systemgedanke hier jedoch überzeugt, wird hier im Ergebnis eine teleologische Reduktion des Art. 32 Abs. 2 DS-GVO befürwortet.

Aufgrund der fehlenden Entscheidungsrelevanz für diese Arbeit wird aus Gründen der Einfachheit und besseren Darstellung künftig – sofern es um die Regelungszwecke des Art. 32 DS-GVO geht – auf den Schutz vor personal data breaches verwiesen.

## D. Einschränkung auf das Risiko für betroffene Personen

Der Schutz vor Sicherheitsvorfällen bzw. konkret der Schutz vor einem personal data breach wirft jedoch ein neues Licht auf Art. 32 Abs. 1 DS-GVO. Aus den hier genannten Gründen überzeugt die Auslegung, dass sich der Anwendungsbereich des Art. 32 Abs. 1 DS-GVO auf den Schutz vor einem personal data breach beschränkt.<sup>108</sup> Diese Auslegung könnte allerdings mit dem Verweis auf ein, dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau in Art. 32 Abs. 1 DS-GVO problematisch sein.

Denn der Wortlaut stellt allgemein auf „*Rechte und Freiheiten* natürlicher *Personen*“<sup>109</sup> (Englisch: „*natural persons*“)<sup>110</sup> ab und beschränkt sich sprachlich damit nicht auf betroffene Personen (i.S.d. Art. 4 Nr. 1 DS-GVO). Noch weiter dürfte sogar die niederländische Sprachfassung gehen. Diese spricht nur von „*personen*“. Zwar kann eine betroffene Person i.S.d. Art. 4 Nr. 1 DS-GVO nur eine natürliche Person sein. Dennoch differenziert die Datenschutz-Grundverordnung an anderen Stellen und bei ähnlichen Begriffen zwischen der betroffenen Person und einer natürlichen Person. Andere, ähnliche Begriffe sind bspw.

<sup>108</sup> Siehe hierzu: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle*.

<sup>109</sup> Hervorhebung durch Verfasser.

<sup>110</sup> Französisch: „*personnes physiques*“, Spanisch: „*personas físicas*“, Italienisch: „*persone fisiche*“, Niederländisch: „*personen*“.



in Art. 10 DS-GVO „Rechte und Freiheiten der betroffenen Personen“<sup>111</sup>, in Art. 15 Abs. 4 DS-GVO „Rechte und Freiheiten anderer Personen“<sup>112</sup>, in Art. 4 Nr. 24 DS-GVO „Grundrechte und Grundfreiheiten der betroffenen Personen“<sup>113</sup>, in Art. 22 Abs. 2 lit. b) DS-GVO „Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person“<sup>114</sup> und in Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person“<sup>115</sup>.

Mit Blick auf die Ziele von Art. 32 Abs. 1 DS-GVO dürfte eine Ausweitung auf sämtliche, natürliche Personen oder sogar auf sämtliche Personen (wie die niederländische Sprachfassung dies nahelegt) hingegen nur schwer vereinbar sein. Das Ziel von Art. 32 Abs. 1 DS-GVO ist es, Sicherheitsvorfälle während der Verarbeitung personenbezogener Daten zu verhindern, da hierdurch die Daten auf eine Art und Weise verarbeitet werden, die ursprünglich nicht vorgesehen war und somit die Schutzziele des Datenschutzrechts tangieren.<sup>116</sup> Durch die unplanmäßige Verarbeitung personenbezogener Daten aufgrund von Si-

---

<sup>111</sup> Englisch: „rights and freedoms of data subjects“, Französisch: „les droits et libertés des personnes concernées“, Spanisch: „los derechos y libertades de los interesados“, Italienisch: „i diritti e le libertà degli interessati“, Niederländisch: „de rechten en vrijheden van de betrokkenen“.

<sup>112</sup> Englisch: „rights and freedoms of others“, Französisch: „droits et libertés d'autrui“, Spanisch: „los derechos y libertades de otros“, Italienisch: „i diritti e le libertà altrui“, Niederländisch: „de rechten en vrijheden van anderen“.

<sup>113</sup> Englisch: „the fundamental rights and freedoms of data subjects“, Französisch: „les libertés et droits fondamentaux des personnes concernées“, Spanisch: „los derechos y libertades fundamentales de los interesados“, Italienisch: „diritti e alle libertà fondamentali degli interessati“, Niederländisch: „de grondrechten en de fundamentele vrijheden van betrokkenen“.

<sup>114</sup> Englisch: „data subject's rights and freedoms and legitimate interests“, Französisch: „droits et libertés et des intérêts légitimes de la personne concernée“, Spanisch: „los derechos y libertades y los intereses legítimos del interesado“, Italienisch: „dei diritti, delle libertà e dei legittimi interessi dell'interessato“, Niederländisch: „de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene“.

<sup>115</sup> Englisch: „the interests or fundamental rights and freedoms of the data subject“, Französisch: „les intérêts ou les libertés et droits fondamentaux de la personne concernée“, Spanisch: „los intereses o los derechos y libertades fundamentales del interesado“, Italienisch: „gli interessi o i diritti e le libertà fondamentali dell'interessato“, Niederländisch: „de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene“.

<sup>116</sup> Siehe zur Herleitung dieses Ziels: Kap. 4, C. Personal data breaches (und andere Sicherheitsvorfälle).

cherheitsvorfällen können aber nur die Rechtsgüter der Personengruppen betroffen sein, die zuvor von der Verarbeitung der personenbezogenen Daten betroffen waren. Die Rechte anderer natürlicher Personen würden bei dieser Zielsetzung nicht dem Schutzbereich der Vorschrift unterfallen.

Dies müsste erst recht gelten, würde man den noch weiteren Begriff der niederländischen Sprachfassung zugrunde legen. Eine Ausweitung auf sämtliche Personen (und damit auch juristische Personen) dürfte schon allein mit dem Anwendungsbereich der Datenschutz-Grundverordnung wohl kaum zu vereinbaren sein. Nach Art. 1 DS-GVO bezieht sich der Schutz der Verordnung ausschließlich auf natürliche Personen, was sich letztlich auch in der Definition der „personenbezogenen Daten“ nach Art. 4 Nr. 1 DS-GVO als zentralen Anknüpfungspunkt<sup>117</sup> der Datenschutz-Grundverordnung widerspiegelt und umfasst damit gerade nicht den Schutz juristischer Personen.<sup>118</sup>

Ausgehend von dem Ziel von Art. 32 DS-GVO kann es folglich also nur um die betroffenen Personen i.S.d. Art. 4 Nr. 1 DS-GVO gehen.<sup>119</sup>

---

<sup>117</sup> Zum Begriff als zentralen Anknüpfungspunkt für die Datenschutz-Grundverordnung: Simitis/Hornung/Spiecker gen. Döhmann/Karg, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO, Rn. 1; Paal/Pauly/Ernst, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 DS-GVO, Rn. 3; Spiecker gen. Döhmann u.a./Farinbo, GDPR, 2023, Art. 4(1) GDPR, Rn. 1, „key concept“; Wybitul/Pötters/Böhm, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 4 DS-GVO, Rn. 7, „Schlüssel zur DSGVO“; Moos/Schefzig/Arning/Moos, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 2, Rn. 10 f.; Gierschmann u.a./Buchholtz/Stentzel, Datenschutz-Grundverordnung, 2018, Art. 4 Nr. 1 DS-GVO, Rn. 1; Hofmann/Johannes, ZD 2017, S. 221, 222; Kuner/Bygrave/Docksey/Bygrave/Tosoni, GDPR, 2020, p. 105, zur Bedeutung für die Datenschutz-Grundverordnung und allgemein für das Datenschutzrecht; siehe auch allgemein als zentrale Frage des Datenschutzrechts: Boehme-Neßler, DuD 2016, S. 419, 419 f., zum Begriff der personenbezogenen Daten und dem Personenbezug als „Schlüsselbegriff des Datenschutzrechts“, mit Verweis auf Saeltzer, DuD 2004, S. 218, 218, „Gretchenfrage des Datenschutzes“; ähnlich Specht-Riemenschneider/Werry/Werry/Schmidt, Datenrecht in der Digitalisierung, 2020, § 2.1, Rn. 8.

<sup>118</sup> EuGH, Rs. C-620/19 (J & S Service), ECLI:EU:C:2020:1011 = ZD 2021, S. 319, Rn. 41; Simitis/Hornung/Spiecker gen. Döhmann/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 1 DS-GVO, Rn. 39; Gola/Heckmann/Pötters, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 1 DS-GVO, Rn. 8; Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 36.

<sup>119</sup> Siehe auch Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 38, die dies aus dem allgemeinen Ziel des Schutzes betroffener Personen und dem Anwendungsbereich der Datenschutz-Grundverordnung herleiten.

Auch in der Literatur scheint man sich mit dem Verweis auf die Rechte und Freiheiten *natürlicher* Personen schwer zu tun. Geht es um die Auseinandersetzung mit dem konkreten Wortlaut, so wird zwar darauf verwiesen, dass Art. 32 Abs. 1 DS-GVO nicht auf die Rechte und Freiheiten betroffener Personen beschränkt sei, sondern auch andere natürliche Personen umfasse.<sup>120</sup> Eine überzeugende Erklärung, in welchen Konstellationen dies relevant werden könnte und warum Art. 32 Abs. 1 DS-GVO den Anwendungsbereich hier (vermeintlich) erweitert, erfolgt – soweit ersichtlich – nicht. Geht es nicht speziell um den Wortlaut, wird hingegen vielfach nur auf die betroffenen Personen als Personenkreis Bezug genommen.<sup>121</sup> Ob dies aus Einfachheitsgründen erfolgt oder eine Wertung darstellen soll, ist allerdings nicht ersichtlich. Soweit erkennbar, wurde diese Frage im Zusammenhang mit Art. 32 DS-GVO bislang nicht tiefer erörtert.<sup>122</sup>

Weitere Anhaltspunkte darauf, welchen Personenkreis Art. 32 Abs. 1 DS-GVO schützen möchte, könnten sich aus der Systematik ergeben. Der mit Art. 32 DS-GVO verwandte<sup>123</sup> Art. 34 Abs. 1 DS-GVO verweist auf „*ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen*“<sup>124</sup>.

<sup>120</sup> Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 29, wonach es sich „*nicht bereits um betroffene Personen handeln*“ muss; Jahnelt/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 14, mit dem Verweis auf den Wortlaut „*natürliche Personen*“, dass es „*primär, aber nicht ausschließlich*“ um die betroffenen Personen geht; a.A. Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 38, mit Kritik am zu weiten Wortlaut.

<sup>121</sup> Vgl. Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 4; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 48; Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 32; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 85, 106; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3; Gärtner/Selzer, DuD 2023, S. 289, 290; Suwelack, ZD 2020, S. 561, 563; Gossen/Schramm, ZD 2017, S. 7, 13; Sundermann, DuD 2021, S. 594, 594.

<sup>122</sup> Siehe jedoch Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 38, eben mit der Kritik am zu weiten Wortlaut und der Einschränkung auf betroffene Personen mit Verweis auf Ziel und Anwendungsbereich der Datenschutz-Grundverordnung.

<sup>123</sup> Siehe hierzu: Kap. 4, C., II. Die Bedeutung des Begriffs „*personal data breach*“.

<sup>124</sup> Englisch: „*a high risk to the rights and freedoms of natural persons*“, Französisch: „*un risque élevé pour les droits et libertés d'une personne physique*“, Spanisch: „*un alto riesgo para los derechos y libertades de las personas físicas*“, Italienisch: „*un rischio elevato per i diritti e le libertà*“.

Art. 34 DS-GVO umfasst die Benachrichtigungspflicht über einen personal data breach gegenüber der betroffenen Person, wenn ein personal data breach voraussichtlich ein hohes Risiko für die (persönlichen) Rechte und Freiheiten natürlicher Personen zur Folge hat.

Ob trotz der bereits festgestellten Nähe<sup>125</sup> ein Vergleich beider Vorschriften möglich ist, bedarf jedoch vorab einer genaueren Untersuchung. Zunächst fällt auf, dass der Begriff in Art. 34 Abs. 1 DS-GVO von dem des Art. 32 Abs. 1 DS-GVO abweicht. Art. 34 Abs. 1 DS-GVO verweist auf ein „*hohes Risiko*“<sup>126</sup> anstelle eines (einfachen) Risikos, wie es in Art. 32 DS-GVO heißt. Dies dürfte allerdings noch nicht bedeuten, dass die Begriffe in den beiden Vorschriften nicht grds. übereinstimmen und daher vergleichbar wären. Art. 34 Abs. 1 DS-GVO könnte lediglich ein qualifizierteres aber ansonsten mit Art. 32 DS-GVO übereinstimmendes Risiko voraussetzen.

Dass es sich aber möglicherweise um unterschiedliche Risiken handelt, könnte sich aus der deutschen Sprachfassung der Datenschutz-Grundverordnung ergeben. Denn diese spricht in Art. 34 Abs. 1 DS-GVO von einem hohen Risiko für die „*persönlichen Rechte und Freiheiten natürlicher Personen*“<sup>127</sup>. Durch den Zusatz „*persönlichen*“ könnte es sich daher in Art. 34 Abs. 1 DS-GVO nicht nur um eine höhere Qualität des Risikos an sich handeln, sondern dieses hohe Risiko könnte sich auch auf ein abweichendes Schutzgut beziehen.

Im direkten Vergleich weist allerdings keine der untersuchten Sprachfassungen diesen Zusatz auf. So spricht bspw. die englische Fassung von „*rights and freedoms of natural persons*“<sup>128</sup>. Überwiegend verwenden die untersuchten Sprachfassungen damit gleichzeitig die Formulierung wie in Art. 32 Abs. 1 DS-GVO. Beachtlich ist insofern vor allem auch die niederländische Sprachfassung. Denn diese verweist in Art. 34 Abs. 1 DS-GVO gerade nicht – wie noch in Art. 32 Abs. 1 DS-GVO – allgemein auf Personen (Niederländisch: „*personen*“),

---

*delle persone fisiche*“, Niederländisch: „*een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*“.

<sup>125</sup> Siehe hierzu: Kap. 4, C., II. Die Bedeutung des Begriffs „*personal data breach*“.

<sup>126</sup> Englisch: „*a high risk*“, Französisch: „*un risque élevé*“, Spanisch: „*un alto riesgo*“, Italienisch: „*un rischio elevato*“, Niederländisch: „*een hoog risico*“.

<sup>127</sup> Hervorhebung durch Verfasser.

<sup>128</sup> Französisch: „*les droits et libertés d'une personne physique*“, Spanisch: „*los derechos y libertades de las personas físicas*“, Italienisch: „*i diritti e le libertà delle persone fisiche*“, Niederländisch: „*de rechten en vrijheden van natuurlijke personen*“.

sondern spricht nun auch von natürlichen Personen (Niederländisch: „*natuurlijke personen*“). Einen weitergehenden Zusatz, der sich wie in der deutschen Fassung auf „*persönliche Rechte und Freiheiten*“<sup>129</sup> bezieht, kennt aber auch die niederländische Sprachfassung nicht (vgl. Niederländisch: „*de rechten en vrijheden van natuurlijke personen*“).

Soweit ersichtlich wird in der Diskussion die sprachliche Divergenz zwischen Art. 34 Abs. 1 DS-GVO und bspw. Art. 32 Abs. 1 DS-GVO oder zwischen den verschiedenen Sprachfassungen des Art. 34 Abs. 1 DS-GVO nicht umfassend behandelt.<sup>130</sup> Auffällig ist allerdings, dass in der Literatur abseits von dem konkreten Wortlaut häufig nur von einem „*hohen Risiko für die Rechte und Freiheiten*“ gesprochen wird.<sup>131</sup> Ferner wird auch gerade nur der Unterschied des „*hohen Risikos*“ im Vergleich zu Art. 33 DS-GVO – der ebenfalls nur von „*Risiko für die Rechte und Freiheiten natürlicher Personen*“<sup>132</sup> spricht – herausgestellt.<sup>133</sup> Auch unter Beachtung der Verbindung<sup>134</sup> zwischen den Art. 32, 33 und 34 DS-

<sup>129</sup> Hervorhebung durch Verfasser.

<sup>130</sup> Siehe jedoch Jahnelt/*Jahnelt*, DSGVO, 2021, Art. 34 DS-GVO, Rn. 3, der aufgrund eines Sprachvergleichs mit der englischen Fassung der Art. 33 und 34 DS-GVO in dem Zusatz „*persönlichen*“ „*kein[en] relevanten Unterschied bei diesem Tatbestandsmerkmal*“ sieht.

<sup>131</sup> Siehe bspw. Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 34 DS-GVO, Rn. 2; Knyrim/*Zavadil*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 11.41; Simitis/Hornung/Spiecker gen. Döhmman/*Dix*, Datenschutzrecht, 2019, Art. 34 DS-GVO, Rn. 4, spricht sogar (nur) von dem Risiko für die Rechte und Freiheiten „*der betroffenen Person*“; ähnlich Freund u.a./*Sundermann*, DSGVO, 2023, Art. 34 DS-GVO, Rn. 10. Anders Sydow/Marsch/*Wilhelm-Robertson*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 34 DS-GVO, Rn. 5 ff., die durchgehend auf die „*persönlichen Rechte und Freiheiten*“ abstellt, aber ohne auf diesen Zusatz konkret einzugehen.

<sup>132</sup> Englisch: „*risk to the rights and freedoms of natural persons*“, Französisch: „*risque pour les droits et libertés des personnes physiques*“, Spanisch: „*riesgo para los derechos y las libertades de las personas físicas*“, Italienisch: „*rischio per i diritti e le libertà delle persone fisiche*“, Niederländisch: „*risico inhoudt voor de rechten en vrijheden van natuurlijke personen*“.

<sup>133</sup> Siehe hierzu: Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 34 DS-GVO, Rn. 29 f.; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 34 DS-GVO, Rn. 5 f.; Feiler/*Forgó*, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 34 DS-GVO, Rn. 3 f., verweisen für das Risiko auf Art. 33 DS-GVO und ergänzen anschließend die Ausführungen um das „*hohe*“ Risiko; ähnlich Maslewski, ZD 2023, S. 251, 255; Freund u.a./*Sundermann*, DSGVO, 2023, Art. 34 DS-GVO, Rn. 7, 10, 13; DatKomm/*König/Schaupp*, Stand: 76. EL. 2023, Art. 34 DS-GVO (Stand: Mai 2022), Rn. 12, verweisen für die „*Art der Risiken*“ ebenfalls auf Art. 33 DS-GVO.

<sup>134</sup> Siehe hierzu: Kap. 4, C., II. Die Bedeutung des Begriffs „*personal data breach*“.

GVO ist die sprachliche Abweichung der deutschen Fassung nicht verständlich. Bei der Abweichung in der deutschen Sprachfassung des Art. 34 Abs. 1 DS-GVO scheint es sich somit um einen Übersetzungsfehler zu handeln.<sup>135</sup> Ein Vergleich zwischen den beiden Vorschriften ist daher möglich.

Betrachtet man nun Art. 34 DS-GVO, so sprechen sowohl die Überschrift als auch Art. 34 Abs. 1 DS-GVO hier ausdrücklich von der Benachrichtigung an die *betreffene* Person. Für eine Pflicht zur Benachrichtigung der betroffenen Person kann dann aber nicht Voraussetzung sein, dass ein Risiko für (andere) natürliche Personen aus einem personal data breach besteht. Es kann nur auf das Risiko der betroffenen Personen ankommen.<sup>136</sup> Hierfür spricht auch Art. 34 Abs. 3 lit. b) DS-GVO. Art. 34 Abs. 3 DS-GVO beschreibt Ausnahmen von der Benachrichtigungspflicht nach Art. 34 Abs. 1 DS-GVO. Nach dessen lit. b) ist die Benachrichtigung der betroffenen Person nicht erforderlich, wenn der Verantwortliche sichergestellt hat, dass das „hohe Risiko für die Rechte und Freiheiten der betroffenen Personen“<sup>137</sup> nach Abs. 1 wahrscheinlich nicht mehr besteht. Während also Art. 34 Abs. 1 DS-GVO noch allgemein von einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen spricht, verweist Art. 34 Abs. 3 lit. b) DS-GVO auf eben dieses hohe Risiko, spricht dann allerdings (nur) von betroffenen Personen.

Die einzig denkbare Möglichkeit wäre, dass die Verordnung hier vielleicht den Begriff der betroffenen Personen anders auslegen und damit auf die Personen abstellen möchte, die vom personal data breach betroffen sind.

---

<sup>135</sup> Jahn/Jahnel, DSGVO, 2021, Art. 34 DS-GVO, Rn. 3, ohne dies klar als Übersetzungsfehler einzuordnen.

<sup>136</sup> Jahn/Jahnel, DSGVO, 2021, Art. 34 DS-GVO, Rn. 4, verweist daher darauf, dass (zumindest) nach Art. 33, 34 DS-GVO die Begriffe „natürliche Person“ und „betreffene Person“ „synonym verwendet“ werden. Vgl. auch BeckOK Datenschutzrecht/Brink, Stand: 46. Ed. 2023, Art. 34 DS-GVO (Stand: Februar 2022), Rn. 4, der ausdrücklich vom Schutz der „Rechte und Freiheiten des Betroffenen“ spricht; auch Freund u.a./Sundermann, DSGVO, 2023, Art. 34 DS-GVO, Rn. 7, 10 f.; ähnlich Gola/Heckmann/Reif, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 34 DS-GVO, Rn. 4 f.; siehe auch DatKomm/König/Schaupp, Stand: EL. 2023, Art. 34 DS-GVO (Stand: Mai 2022), Rn. 8, mit Verweis auf die betroffene Person als „Adressat der Benachrichtigung“.

<sup>137</sup> Englisch: „high risk to the rights and freedoms of data subjects“, Französisch: „le risque élevé pour les droits et libertés des personnes concernées“, Spanisch: „el alto riesgo para los derechos y libertades del interesado“, Italienisch: „un rischio elevato per i diritti e le libertà degli interessati“, Niederländisch: „hoge risico voor de rechten en vrijheden van betrokkenen“.

Der Begriff der „betroffenen Person“<sup>138</sup> wird hingegen gemeinsam mit dem Begriff der „personenbezogenen Daten“ in Art. 4 Nr. 1 DS-GVO legal definiert.<sup>139</sup> Unter den betroffenen Personen sind demnach die Personen zu verstehen, deren personenbezogene Daten verarbeitet werden.<sup>140</sup> Von einem personal data breach betroffene Personen sind nach der Definition nicht (direkt) erfasst. Insofern gilt zunächst die Vermutung, dass der Begriff innerhalb der Datenschutz-Grundverordnung einheitlich im Sinne dieser Definition zu verstehen ist.<sup>141</sup> Eine – im Wege der funktionalen Auslegung –<sup>142</sup> hiervon abweichende Auslegung bedarf dann aber einer besonderen Begründung.<sup>143</sup> Gegen eine funktionale Auslegung dürfte dabei gerade die englische Sprachfassung sprechen.

---

<sup>138</sup> Englisch: „data subject“, Französisch: „personne concernée“, Spanisch: „el interesado“, Italienisch: „interessato“, Niederländisch: „de betrokkene“.

<sup>139</sup> Sydow/Marsch/Ziebarth, DS-GVO – BDSG, 3. Aufl. 2022, Art. 4 DS-GVO, Rn. 7; Kühling/Buchner/Klar/Kübling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 1 DS-GVO, unter der Überschrift „Nr. 1 personenbezogene Daten (inkl. betroffene Person)“; vgl. auch BeckOK Datenschutzrecht/Schild, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 28, „Klammerzusatz“; Ehmann/Selmayr/Klabunde, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 12, „implizit“ aus der Definition der personenbezogenen Daten; siehe auch Jabnel/Pallwein-Pretzner, Datenschutzrecht, 3. Aufl. 2021, S. 61.

<sup>140</sup> Vgl. BeckOK Datenschutzrecht/Schild, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 28; Gola/Heckmann/Gola, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 4 DS-GVO, Rn. 5; Ehmann/Selmayr/Klabunde, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 12.

<sup>141</sup> Vgl. zur grds. Geltung einer Definition für den gesamten Rechtsakt: Europäische Union, Gemeinsamer Leitfaden für das Abfassung von Rechtstexten, 2015, DOI 10.2880/836230, Leitlinie 14.1.; Jung, Spezifika der europäischen Methodenlehre, in: Das Vorabentscheidungsverfahren in der Zivilgerichtsbarkeit, 2014, S. 17, 21; Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81.

<sup>142</sup> Allgemein zur funktionalen Auslegung in der europäischen Methodik: EuGH, verb. Rs. C-403/08, C-429/08 (Football Association Premier League u.a.), ECLI:EU:C:2011:631 = ZUM 2011, 803, Rn. 187 f.; EuGH, Rs. C-128/11 (UsedSoft), ECLI:EU:C:2012:407 = ZUM 2012, S. 661, Rn. 60; Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81; vgl. auch Riesenhuber/Riesenhuber, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 20, zur „Relativität der Rechtsbegriffe“; Beck, The Legal Reasoning of the Court of Justice of the EU, 2012, p. 192 f.; Müller/Christensen, Juristische Methodik, II. Bd. Europarecht, 3. Aufl. 2012, Rn. 61.

<sup>143</sup> Jung, Spezifika der europäischen Methodenlehre, in: Das Vorabentscheidungsverfahren in der Zivilgerichtsbarkeit, 2014, S. 17, 21; Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81.

Der Begriff für „*betroffene Personen*“ ist in der englischen Fassung „*data subject*“. Auch dieser Begriff wird in Art. 34 DS-GVO zugrunde gelegt.<sup>144</sup> Anders als die deutsche Bezeichnung bezieht sich der englische Begriff noch deutlicher auf Personen, deren personenbezogenen Daten verarbeitet werden. Eine Auslegung dahingehend, dass es sich in Art. 34 DS-GVO um Personen handelt, die von einem personal data breach „betroffen“ sind, ist auf Basis des englischen Begriffs damit schwerer zu vertreten.

Weiterhin könnte sich ein (abweichender) Personenkreis aber auch faktisch nur auf betroffene Personen i.S.d. Art. 4 Nr. 1 DS-GVO beschränken. Denn ein personal data breach zeichnet sich nach Art. 4 Nr. 12 DS-GVO durch eine Verletzung der Sicherheit bei der Verarbeitung personenbezogener Daten aus. Die Definition nach Art. 4 Nr. 12 DS-GVO knüpft damit ebenfalls an die Definition der personenbezogenen Daten und damit gleichzeitig an die Definition der betroffenen Person an. Andere natürliche Personen können demnach nicht von einem personal data breach i.S.d. Art. 4 Nr. 12 DS-GVO betroffen sein.

Aufgrund der bestehenden Systematik aus Art. 4 Nr. 12, Art. 32 bis 34 DS-GVO kann im Ergebnis daher auch für Art. 32 Abs. 1 DS-GVO nur gelten, dass sich der Begriff, solange es um die Ziele von Art. 32 DS-GVO geht,<sup>145</sup> nur auf das, dem Risiko für die Rechte und Freiheiten betroffener Personen angemessene Schutzniveau beschränkt.<sup>146</sup>

---

<sup>144</sup> Französisch: „*personne concernée*“, Spanisch: „*al interesado*“, Italienisch: „*interessato*“, Niederländisch: „*de betrokkene*“.

<sup>145</sup> Dem Begriff könnte eine Doppelfunktion zukommen, die eine abweichende Auslegung gebietet. Ausführlicher hierzu: Kap. 7, B., IV., 2. *Möglichkeit einer Doppelfunktion*.

<sup>146</sup> Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 38; wohl im Ergebnis auch Schneider, Datenschutz, 2. Aufl. 2019, S. 263, der im Zusammenhang des „*Risiko angemessene[n] Schutzniveau[s]*“ knapp auf die „*Rechte der Betroffenen*“ verweist. Siehe auch zum gleichlautenden Begriff in Art. 33 (und Art. 34) DS-GVO Jähnel/Jähnel, DSGVO, 2021, Art. 33 DS-GVO, Rn. 15 und Art. 34 DS-GVO, Rn. 4.



## E. Das Verhältnis zu Art. 32 Abs. 4 DS-GVO

### I. Überschneidungen im Anwendungsbereich

Abschließend ist noch auf Art. 32 Abs. 4 DS-GVO einzugehen. Danach müssen Verantwortliche und Auftragsverarbeiter sicherstellen, dass unterstellte Personen personenbezogene Daten grds. nur nach Anweisung des Verantwortlichen verarbeiten. Hierzu müssen Datenverarbeiter „Schritte unternehmen“<sup>147</sup>, die dies sicherstellen sollen. Abgesehen davon, dass Art. 32 Abs. 4 DS-GVO mit der Verpflichtung „Schritte zu unternehmen“ sehr vage formuliert ist, wirft Absatz 4 aber auch die generelle Frage des Verhältnisses zu Art. 32 Abs. 1 DS-GVO auf.

Vergleicht man die beiden Absätze, fallen einige Aspekte auf. Die Pflicht „Schritte zu unternehmen“ deutet darauf hin, dass Verantwortliche und Auftragsverarbeiter bestimmte Maßnahmen treffen sollen (vgl. insofern auch andere Sprachfassungen, wie die Französische: „prennent des mesures“<sup>148</sup>, die sogar von „Maßnahmen“ sprechen).<sup>149</sup> Hier zeigt sich eine erste Gemeinsamkeit mit Art. 32 Abs. 1 DS-GVO, nach dem Verantwortliche und Auftragsverarbeiter (technische und organisatorische) Maßnahmen treffen müssen.

Weitere Gemeinsamkeiten zeigen sich zudem, wenn man sich anschließend die „Ziele“ anschaut, die mit den Maßnahmen bzw. Schritten erreicht werden sollen. Nach Art. 32 Abs. 4 DS-GVO soll sichergestellt werden, dass personenbezogene Daten von unterstellten Personen grds. nur nach Anweisung des Verantwortlichen verarbeitet werden. In Art. 32 Abs. 1 DS-GVO sollen die Maßnahmen hingegen ein, dem Risiko angemessenes Schutzniveau sicherstellen. Wie oben bereits hervorgehoben wurde, geht es in Art. 32 Abs. 1 DS-GVO darum, eine „ungeplante“ Verarbeitung (i.S.e. personal data breach) personenbezogener Daten zu verhindern.<sup>150</sup> Eine Verarbeitung entgegen den Anweisungen

<sup>147</sup> Englisch: „take steps“, Französisch: „prennent des mesures“, Spanisch: „tomarán medidas“, Italienisch: „Il titolare del trattamento e il responsabile del trattamento fanno sì [...]“, Niederländisch: „treffen maatregelen“.

<sup>148</sup> Spanisch: „tomarán medidas“, Niederländisch: „treffen maatregelen“.

<sup>149</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 67, mit Bezug auf die unterschiedlichen Begriffe; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 37 f.; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 27.

<sup>150</sup> Siehe hierzu ausführlicher: Kap. 4, C. Personal data breaches (und andere Sicherheitsvorfälle).

des Verantwortlichen durch unterstellte Personen, stellt aber auch einen Fall einer solchen „ungeplanten“ Verarbeitung dar. Es handelt sich dann, abhängig von der Art der Verarbeitung um eine Vernichtung, einen Verlust, eine Veränderung, eine Offenlegung von personenbezogenen Daten oder um einen Zugang zu personenbezogenen Daten. Sie wäre daher bereits von Art. 32 Abs. 1 i.V.m. Abs. 2 DS-GVO abgedeckt und müssten im Rahmen des angemessenen Schutzniveaus berücksichtigt werden.

## II. Probleme bei gleichrangiger Verpflichtung

Fraglich ist daher, ob Art. 32 Abs. 4 DS-GVO Verantwortliche und Auftragsverarbeiter eine zusätzliche (?) Pflicht auferlegt, Schritte zu unternehmen, die eine Verarbeitung entgegen den Anweisungen des Verantwortlichen verhindern sollen. Ein solches Nebeneinander von Art. 32 Abs. 1 und Abs. 4 DS-GVO könnte allerdings problematisch sein. Denn ausgehend vom Wortlaut des Art. 32 Abs. 1 DS-GVO verfolgt dieser mit dem „*Risiko angemessenen Schutzniveau*“<sup>151</sup> einen relativen Ansatz, der auf den jeweiligen Einzelfall abstellt.<sup>152</sup> Zwar ist die Pflicht „*Schritte zu unternehmen*“ in Absatz 4 sehr vage beschrieben. Eine klare Relativierung wie nach Art. 32 Abs. 1 DS-GVO fehlt in Absatz 4 allerdings.<sup>153</sup> Theoretisch könnte dies zu divergierenden Pflichten führen.

<sup>151</sup> Englisch: „*level of security appropriate to the risk*“, Französisch: „*un niveau de sécurité adapté au risque*“, Spanisch: „*un nivel de seguridad adecuado al riesgo*“, Italienisch: „*un livello di sicurezza adeguato al rischio*“, Niederländisch: „*op het risico afgestemd beveiligingsniveau*“.

<sup>152</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 46; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11; BeckOK Datenschutzrecht/Paulus, Stand: 46. Ed. 2023, Art. 32 DS-GVO (Stand: November 2021), Rn. 7. Siehe hierzu noch ausführlicher: Kap. 5, B., I. *Bedeutung der Angemessenheit*.

<sup>153</sup> Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 22; Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 43; Katko/Meyer, Checklisten zur Datenschutz-Grundverordnung, 2. Aufl. 2023, § 9, Rn. 57; siehe auch Jähnel/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 18, dass es sich um „*eine zwingende organisatorische Maßnahme*“ handle. A.A. Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 70, die eine „*absolute*“ Gewährleistung mit der Formulierung „*Schritte*“ und dem Verweis auf den allgemeinen risikobasierten Ansatz des Art. 32 DS-GVO ablehnen; ähnlich mit Verweis auf die Formulierung v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 35.

Ob dies vom Gesetzgeber beabsichtigt war, bedarf daher einer näheren Untersuchung. So könnte man argumentieren, dass die Datenschutz-Grundverordnung den Schutz vor Sicherheitsvorfällen in Art. 32 Abs. 1 DS-GVO einmal allgemein und für den spezifischen Schutz vor Verarbeitung entgegen den Anweisungen des Verantwortlichen durch unterstellte Personen noch einmal gesondert in Art. 32 Abs. 4 DS-GVO regeln wollte. In diesem Fall hätte man aber erwarten dürfen, dass in Art. 32 Abs. 4 DS-GVO auch spezifische Pflichten für diesen – dann ja wohl zwingenden und herausgestellten – Spezialfall benannt werden. Hieran fehlt es allerdings.

Aus der Entstehungsgeschichte<sup>154</sup> von Art. 32 Abs. 4 DS-GVO könnten sich Anhaltspunkte ergeben, wie dessen Verhältnis zu Art. 32 Abs. 1 DS-GVO zu

---

<sup>154</sup> Zur Berücksichtigung der Entstehungsgeschichte im Rahmen der Europäischen Auslegung: EuGH, Rs. C-337/20 (CRCAM), ECLI:EU:C:2021:671 = BeckRS 2021, 24493, Rn. 31, 47 ff.; EuGH, Rs. C-135/15 (Nikiforidis), ECLI:EU:C:2016:774 = NJW 2017, S. 141, Rn. 34; EuGH, Rs. C-203/09 (Volvo Car Germany), ECLI:EU:C:2010:647 = NJW-RR 2011, S. 255, Rn. 40. Als Teil der historischen/genetischen Auslegung: Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 32 ff.; Höpfner/*Rüthers*, AcP 209 (2009), S. 1, 13 ff.; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 125; Roth, RabelsZ 75 (2011), S. 787, 800; Leisner, EuR 2007, S. 689, 689 ff, insb. 698 ff.; Martens, Methodenlehre des Unionsrechts, 2013, S. 391 f.; Henninger, Europäisches Privatrecht und Methode, 2009, S. 288, mit Verweis, dass die historische Auslegung im EU-Recht der Auslegung nach dem Gesetzeszweck untergeordnet sei (S. 287). Die Entstehungsgeschichte soll allerdings nur zu berücksichtigen sein, wenn die Dokumente auch veröffentlicht wurden: Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 36 f.; Henninger, Europäisches Privatrecht und Methode, 2009, S. 288 f.; Martens, Methodenlehre des Unionsrechts, 2013, S. 392 f.; vgl. Roth, RabelsZ 75 (2011), S. 787, 800, der gerade auf die geringe Bedeutung der historischen Auslegung im Primärrecht verweist, weil es dort lange an veröffentlichten Dokumenten fehlte; ähnlich Höpfner/*Rüthers*, AcP 209 (2009), S. 1, 14; weiter wohl Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 126, die nicht nur Dokumente berücksichtigen wollen, die veröffentlicht wurden, sondern auch solche, die „auf Antrag einsehbar sind“; ähnlich auch Leisner, EuR 2007, S. 689, 695 ff., der eine „generelle Unbeachtlichkeit [...] nicht veröffentlichter Dokumente“ ablehnt.

verstehen ist. Art. 32 Abs. 4 DS-GVO wurde während des Gesetzgebungsverfahrens erst vom Rat aufgenommen.<sup>155</sup> In seinen Dokumenten weist der Rat darauf hin, dass der Wortlaut aus Art. 16 DS-RL übernommen wurde.<sup>156</sup> Die Aussage des Rats, es handele sich hierbei um eine Übernahme des Wortlauts aus der Datenschutzrichtlinie, ist aber irreführend. Der Wortlaut ist nicht identisch.<sup>157</sup> Art. 16 DS-RL ist nämlich weniger als eine Verpflichtung des Verantwortlichen (und wenn man dies auf Art. 32 Abs. 4 DS-GVO übertragen würde, auch des Auftragsverarbeiters) ausgestaltet. Die Regelung adressiert vielmehr die unterstellten Personen und den Auftragsverarbeiter direkt und ordnet an, dass personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeitet werden dürfen. Weiterhin war die Regelung in der Datenschutzrichtlinie noch nicht Teil der Sicherheit der Verarbeitung, denn diese wurde erst in Art. 17 DS-RL geregelt.

Mit der Datenschutz-Grundverordnung haben sich hier nun einige wesentliche Punkte „geändert“. Zunächst wird in Art. 32 Abs. 4 DS-GVO der Auftragsverarbeiter selbst nicht mehr auf seine Weisungsgebundenheit verpflichtet, sondern Art. 32 Abs. 4 DS-GVO stellt (nur noch) auf die unterstellten (aber auch die dem Auftragsverarbeiter unterstellten) Personen ab. Dass der Auftragsverarbeiter hier herausgenommen wurde, verwundert allerdings nicht. Denn das Verhältnis zwischen Auftragsverarbeiter und Verantwortlichen wurde in der Datenschutz-Grundverordnung im Vergleich zur früheren Datenschutzrichtlinie deutlich ausgebaut (vgl. Art. 28 DS-GVO).<sup>158</sup> Dass der Auf-

---

<sup>155</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013, S. 82, Art. 30 Abs. 2b; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 49.

<sup>156</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013, S. 82, Fn. 230; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 49.

<sup>157</sup> Vgl. Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 49, „fast identisch“.

<sup>158</sup> BeckOK Datenschutzrecht/*Spoerr*, Stand: 46. Ed. 2023, Art. 28 DS-GVO (Stand: Mai 2022), Rn. 6; Kühling/Buchner/*Hartung*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 28 DS-GVO, Rn. 4 f.; Sydow/Marsch/*Ingold*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 28 DS-GVO, Rn. 11.

tragsverarbeiter dabei den Weisungen des Verantwortlichen bei der Verarbeitung der personenbezogenen Daten unterstellt ist, ergibt sich bereits aus deren Verhältnis (vgl. Art. 4 Nr. 8, Art. 28, Art. 29 DS-GVO).<sup>159</sup>

Im Lichte des Art. 32 Abs. 4 DS-GVO ist aber vor allem Art. 29 DS-GVO zu beachten. Ähnlich wie Art. 32 Abs. 4 DS-GVO stellt auch Art. 29 DS-GVO klar, dass (diesmal auch) Auftragsverarbeiter und dem Verantwortlichen oder Auftragsverarbeiter unterstellten Personen, personenbezogene Daten grds. nur auf Weisung des Verantwortlichen verarbeiten dürfen. Damit entspricht Art. 29 DS-GVO sinngemäß dem früheren Art. 16 DS-RL.<sup>160</sup> Art. 29 DS-GVO war damals bereits als Art. 27 DS-GVO-E (KOM)<sup>161</sup> Teil des ursprünglichen Kommissionsvorschlags gewesen. Im Rahmen einer ersten Überprüfung des Kommissionsvorschlags durch den Rat vom 06.05.2013,<sup>162</sup> haben einige Ratsvertreter den Mehrwert von Art. 27 DS-GVO-E(KOM) in einer Fußnote in Frage gestellt und darauf verwiesen, man habe u.a. die Vertraulichkeitspflichten aus Art. 27 DS-GVO-E(KOM) in Art. 30 DS-GVO-E(RAT)<sup>163</sup> (heute Art. 32 DS-GVO) verschoben.<sup>164</sup> Der Text von Art. 27 DS-GVO-E(KOM) wurde in diesem Ratsdokument durch „(...)“ ersetzt (vgl. Art. 27 DS-GVO-E(RAT)<sup>165</sup>).

---

<sup>159</sup> Ehmann/Selmayr/Bertermann, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 28 DS-GVO, Rn. 3; Gola/Heckmann/Gola, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 4 DS-GVO, Rn. 91; Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 28 DS-GVO, Rn. 11; Sander, PinG 2017, S. 250, 250, beschreibt die Weisungsgebundenheit als „[d]as Wesen der Auftragsverarbeitung“; ähnlich Schulze/Jansen/Kadelbach/Holzner/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 18.

<sup>160</sup> Ehmann/Selmayr/Bertermann, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 29 DS-GVO, Rn. 1; Kühling/Buchner/Hartung, DS-GVO – BDSG, 4. Aufl. 2024, Art. 29 DS-GVO, Rn. 3; Taeger/Gabel/Lutz/Gabel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 29 DS-GVO, Rn. 3; Simitis/Hornung/Spiecker gen. Döhmman/Petri, Datenschutzrecht, 2019, Art. 29 DS-GVO, Rn. 2.

<sup>161</sup> Europäische Kommission, Kommissionsentwurf der DS-GVO, KOM(2012) 11 endgültig, vom 25.01.2012.

<sup>162</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013.

<sup>163</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013.

<sup>164</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013, S. 79, Fn. 214.

<sup>165</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013.

Nach den einleitenden Erklärungen des Rats soll dies bedeuten, dass der Kommissionstext gelöscht wurde.<sup>166</sup>

Mit Ausnahme der Fußnotenerklärung wurde diese Änderung auch im finalen Entwurf des Rats<sup>167</sup> vom 11.06.2015 beibehalten. Zwar enthält der finale Ratsentwurf der Datenschutz-Grundverordnung keine Legende mehr darüber, wie die Änderungen des Rats zu verstehen sind. Ausgehend von den Erklärungen im Rahmen seiner ersten Überprüfung des Kommissionstextes kann man aber wohl davon ausgehen, dass der Rat Art. 27 DS-GVO-E(KOM) gestrichen hat und dafür einen entsprechenden Zusatz in Art. 30 Abs. 2b DS-GVO-E(RAT)<sup>168</sup> aufgenommen hat.<sup>169</sup> Wie bereits angesprochen, wurde dieser Zusatz im Vergleich zum damaligen Art. 27 DS-GVO-E(KOM) umformuliert.

Das Parlament hat auf Basis des Kommissionsvorschlags Art. 27 DS-GVO-E(KOM) ohne Änderungsvorschlag belassen.<sup>170</sup> Im Rahmen der anschließenden Trilog-Verhandlungen wurden daher beide Vorschriften Teil des finalen Verordnungstextes.

Der Unterschied zwischen Art. 32 Abs. 4 DS-GVO zu Art. 29 DS-GVO (und Art. 16 DS-RL) besteht in der direkten Verpflichtung gegenüber dem Verantwortlichen und dem Auftragsverarbeiter. Dass die Datenschutz-Grundverordnung eine wohl gesonderte Verpflichtung formuliert, könnte durch die klarere Zuweisung der Verantwortung (vor allem) des Verantwortlichen innerhalb der Datenschutz-Grundverordnung begründet sein. Vielfach hebt die Datenschutz-Grundverordnung hervor, dass der Verantwortliche dafür zu sorgen hat, dass die Bestimmungen der Datenschutz-Grundverordnung einzuhalten sind und dass er dies nachzuweisen hat (vgl. Art. 5 Abs. 2, Art. 24 DS-GVO).<sup>171</sup>

---

<sup>166</sup> Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013, S. 2, Nr. 4.

<sup>167</sup> Rat der Europäischen Union, Ratsentwurf der DS-GVO, Ratsdokument 9565/15, vom 11.06.2015.

<sup>168</sup> Rat der Europäischen Union, Ratsentwurf der DS-GVO, Ratsdokument 9565/15, vom 11.06.2015.

<sup>169</sup> Vgl. jeweils Art. 27 und 30 DS-GVO-E in: Rat der Europäischen Union, Ratsentwurf der DS-GVO, Ratsdokument 9565/15, vom 11.06.2015.

<sup>170</sup> Europäisches Parlament, Parlamentsentwurf der DS-GVO, P7\_TA(2014)0212, vom 12.03.2014.

<sup>171</sup> Siehe zur Einschätzung der Stärkung der Rechenschaftspflichten des Verantwortlichen durch die Datenschutz-Grundverordnung: Ehmann/Selmayr/Heberlein, Datenschutz-Grund-

Die Zuweisung der Verantwortlichkeit und die Verpflichtung des Verantwortlichen (und des Auftragsverarbeiters) sicherzustellen, dass Verarbeitungen nur entsprechend den Anweisungen des Verantwortlichen zu erfolgen haben, charakterisieren die Vorschrift zwar richtigerweise als eine Regelung der Sicherheit der Verarbeitung. Denn eine Verarbeitung entgegen den Anweisungen stellt, wie schon gesagt, nichts anderes als einen Sicherheitsvorfall dar. Die Eingliederung in Art. 32 DS-GVO ist aus systematischer Sicht daher richtig.

Selbst wenn man unterstellt, der Gesetzgeber wollte hier gezielt Art. 32 Abs. 4 DS-GVO neben Art. 29 DS-GVO regeln,<sup>172</sup> dürfte dem Gesetzgeber bei seiner Überarbeitung entgangen sein, dass er hiermit Gefahr läuft, eine Konkurrenzregel zu Art. 32 Abs. 1 DS-GVO zu schaffen. Dass dies aber wohl gerade nicht beabsichtigt war, lässt sich aus der sehr vage formulierten „Verpflichtung“ des Art. 32 Abs. 4 DS-GVO entnehmen. Weiterhin ergibt es auch aus teleologischen Erwägungen keinen Sinn, eine zusätzliche Verpflichtung in Art. 32 Abs. 4 DS-GVO zu schaffen, die droht, den Anwendungsbereich des Art. 32 Abs. 1 DS-GVO (teilweise) auszuhöhlen.

Dies lässt sich auch nicht – wie wohl in Teilen der Literatur – damit erklären, dass die Pflicht nach Art. 32 Abs. 1 DS-GVO eher auf die technische Perspektive abstelle und Art. 32 Abs. 4 DS-GVO dann die Personelle regele.<sup>173</sup>

---

verordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 29 ff.; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 2, Kapitel 3, Rn. 1 ff.; Roßnagel/Blazy, Das neue Datenschutzrecht, 2018, § 5, Rn. 1; Mester, Informationelle Selbstbestimmung in Zeiten der Datenschutz-Grundverordnung, in: FS Taeger, 2020, S. 291, 294; Jung, ZD 2018, S. 208, 208; Veil, ZD 2018, S. 9 ff. kritisch bzgl. einer umfassenden Rechenschafts- und Nachweispflicht und mit einer Untersuchung über ihre Reichweite, siehe auch seine Untersuchung in Forgó/Helfrich/Schneider/Veil, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil II, Kapitel 1, Rn. 1 ff.

<sup>172</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 66, die Art. 32 Abs. 4 DS-GVO als „prozedurale Entsprechung“ des Art. 29 DS-GVO sieht; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 29 DS-GVO, Rn. 3, wonach Art. 32 Abs. 4 DS-GVO den Art. 29 DS-GVO mit einer „verfahrensrechtlich-organisatorischen Gewährleistungspflicht [flankiert]“; Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 29 DS-GVO, Rn. 6, als „[k]orrespondierend[e]“ „Pflicht zu technisch-organisatorischen Vorkehrungen“ durch Art. 32 DS-GVO; ähnlich Kühling/Buchner/Hartung, DS-GVO – BDSG, 4. Aufl. 2024, Art. 29 DS-GVO, Rn. 2.

<sup>173</sup> So wohl Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 37; ähnlich Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 25; DatKomm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 49.

Zum einen umfasst Art. 32 Abs. 1 DS-GVO mit den organisatorischen Maßnahmen gleichfalls Maßnahmen, die auf personeller Ebene wirken.<sup>174</sup> Ähnlich schließt Art. 32 Abs. 4 eine Umsetzung mit technischen Maßnahmen ebenfalls nicht aus.<sup>175</sup> Zum anderen knüpft Art. 32 Abs. 1 i.V.m. Abs. 2 DS-GVO allgemein an die Sicherheit der Verarbeitung personenbezogener Daten an. Sie begrenzt sich daher nicht auf den technischen Bereich, sondern regelt die Sicherheit umfassend.

Unter Berücksichtigung des Art. 32 Abs. 1 DS-GVO sollte daher – um Konkurrenzprobleme zwischen den Absätzen zu vermeiden – Art. 32 Abs. 4 DS-GVO als eine Art Klarstellung angesehen werden, dass auch Verarbeitungen entgegen den Anweisungen des Verantwortlichen sicherheitsrelevante Bedeutung haben und demnach im Rahmen des Art. 32 Abs. 1 DS-GVO zu beachten sind.<sup>176</sup>

---

<sup>174</sup> Siehe zudem für vergleichbare Beispiele zu organisatorischen Maßnahmen sowohl nach Absatz 1 und 4: Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 26 und 116, „Schulung“; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 37, „interne Handlungsanweisungen an Beschäftigte“ und Rn. 73 „Arbeitsanweisungen“.

<sup>175</sup> Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 27; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 51; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 116 f.; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 70 f.; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 66.

<sup>176</sup> Im Ergebnis wohl auch Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 21, 82, die Art. 32 Abs. 4 DS-GVO in den Kontext der Beispiele nach Art. 32 Abs. 1 Hs. 2 lit. a)-d) DS-GVO (hierzu ausführlicher: Kap. 5, C., IV. Anforderungen an die Maßnahmen nach Art. 32 Abs. 1 Hs. 2 DS-GVO) setzen; ähnlich auch Wennemann, DuD 2018, S. 174, 176, der sowohl bei Art. 32 Abs. 4 als auch bei den Beispielen i.S.d. Art. 32 Abs. 1 Hs. 2 lit. b) und c) DS-GVO von „konkrete[n] Maßnahmenforderungen“ spricht. A.A. Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 22; Weth u.a./Overkamp/Overkamp, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Teil. B., IV., Rn. 43; Jahnelt/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 18; vgl. Katko/Meyer, Checklisten zur Datenschutz-Grundverordnung, 2. Aufl. 2023, § 9, Rn. 57.



## F. Zwischenergebnis und grafische Darstellung

Wie sich anhand einer ersten Betrachtung des Art. 32 DS-GVO gezeigt hat, lassen sich die Regelungsziele nicht so einfach aus der Vorschrift ablesen. Aufgrund einiger ungenauer Begriffe – die sich teilweise nur auf einzelne Sprachfassungen beziehen – wird dem Rechtsanwender der Einstieg in die Vorschrift erschwert. Ferner bedarf es eines grundlegenden Verständnisses über das System, in das Art. 32 DS-GVO innerhalb der Verordnung eingebettet ist, um sich die allgemeinen Regelungsziele zu erschließen.

Im Kern lässt sich sagen, dass Art. 32 DS-GVO betroffene Personen bei der Verarbeitung ihrer Daten vor Sicherheitsvorfällen in Form eines personal data breach schützen möchte.

Zur besseren Veranschaulichung soll das System von der Sicherheit der Verarbeitung nach Art. 32 Abs. 1 und Abs. 2 DS-GVO noch einmal grafisch dargestellt werden:

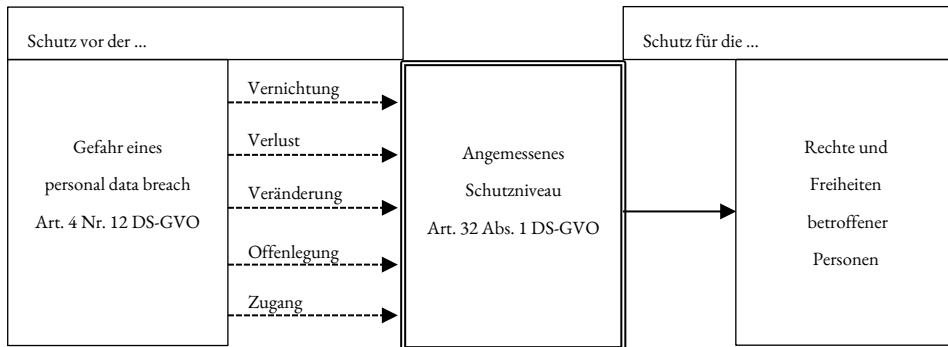


Abb. 1: System der Sicherheit der Verarbeitung nach Art. 32 DS-GVO (eigene Darstellung)



## Kapitel 5

# Anforderungen an die Sicherheit

Die Frage nach den Anforderungen an die Sicherheit der Verarbeitung aus Art. 32 DS-GVO ist entscheidend für die Bewertung datenverarbeitender TOM. Der beschriebene Konflikt bei diesen Sicherheitsmaßnahmen richtet sich auf der einen Seite danach, ob die Sicherheit der Verarbeitung zur Implementierung datenverarbeitender TOM verpflichtet. Abhängig davon, wie die Pflichten in Art. 32 DS-GVO strukturiert sind, können erst Überlegungen zur Lösung des Konflikts angestellt werden. Ausgehend von Art. 32 DS-GVO legt die Vorschrift bei der Bestimmung der Anforderungen an die Sicherheit der Verarbeitung eine 3-Stufen-Prüfung zugrunde.

### A. Risikobewertung

Art. 32 Abs. 1 DS-GVO verpflichtet Verantwortliche und Auftragsverarbeiter zur Gewährleistung eines, dem Risiko angemessenes Schutzniveaus. Die systematische Analyse hat gezeigt, dass es um das Risiko für die Rechte und Freiheiten betroffener<sup>1</sup> Personen durch personal data breaches<sup>2</sup> geht.<sup>3</sup> Art. 32 Abs. 1 DS-GVO richtet sich somit nach dem Risiko der jeweiligen Verarbeitung aus.<sup>4</sup>

---

<sup>1</sup> Anders als der Wortlaut vermuten lässt, beschränkt sich die Anwendung auf betroffene Personen und nicht allgemein auf natürliche Personen, siehe hierzu: Kap. 5, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>2</sup> Nach dem Wortlaut beschränkt sich der Schutz nicht nur auf personal data breaches. Allerdings sollte eine teleologische Reduktion in Betracht gezogen werden, vgl. insgesamt hierzu: Kap. 4, C. Personal data breaches (*und andere Sicherheitsvorfälle*).

<sup>3</sup> Siehe hierzu ausführlich: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO*.

<sup>4</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 46, 48; Jahnelt/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 6; Sundermann, DuD 2021, S. 594,

Zunächst müssen daher die individuell geltenden Anforderungen an die Sicherheit der Verarbeitung bestimmt werden.

Auf der ersten Stufe ist eine Risikobewertung erforderlich.<sup>5</sup> Hierbei ist das Risiko für die Rechte und Freiheiten betroffener Personen durch einen personal data breach bei der Verarbeitung ihrer personenbezogenen Daten zu bewerten.<sup>6</sup> Zu Beginn müssen die Wahrscheinlichkeiten des Eintritts (hier: eines personal data breach) und die dadurch drohenden Folgen für die Rechte und Freiheiten der betroffenen Personen bestimmt werden.<sup>7</sup> Anschließend ist zu bewerten, wie hoch das Risiko ist. Anhand dieser Bewertung richten sich dann die weiteren Anforderungen an die Sicherheit der Verarbeitung.

Die Sicherheit der Verarbeitung setzt damit in ihrem wesentlichen Anknüpfungspunkt eine Einzelfallprüfung voraus. Die jeweilige Verarbeitung muss auf

---

594; Ehmann/Selmayr/*Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 11.

<sup>5</sup> Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 29; Kuner/Bygrave/Docksey/*Burton*, GDPR, 2020, p. 635; Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 8; *Johannes/Geminn*, InTeR 2021, S. 140, 141; Ehmann/Selmayr/*Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 11, spricht von „Schutzbedarfsfeststellung“; so auch Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 48; *Frisse* u.a., BKR 2018, S. 177, 182.

<sup>6</sup> Vgl. die folgenden Nachweise, wobei diese wohl gerade auf die beispielhafte Aufzählung in Art. 32 Abs. 2 DS-GVO verweisen, welche hier kritisiert wird (Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle*): Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 31; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58; Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 23; Kuner/Bygrave/Docksey/*Burton*, GDPR, 2020, p. 635.

<sup>7</sup> Vgl. allgemein, dass es dabei auf die Eintrittswahrscheinlichkeit und die Schwere ankommt: Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 23; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 50 ff.; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 29; Spiecker gen. Döhmann u.a./*Papadaki/Stalla-Bourdillon*, GDPR, 2023, Art. 32 GDPR, Rn. 16; *Ritter/Reibach/Lee*, ZD 2019, S. 531, 533, allgemein zur Risikobewertung innerhalb der Datenschutz-Grundverordnung.

mögliche Gefahren eines personal data breach untersucht und bewertet werden.<sup>8</sup> Mit Blick auf Art. 32 DS-GVO ist hierbei zu beachten, dass sich die Sicherheit auf die gesamte Verarbeitung bezieht.<sup>9</sup> Komplexe Verarbeitungsstrukturen können daher die Risikobewertung weiter erschweren. Dieser Ansatz muss bei der Lösung datenverarbeitender TOM zwar berücksichtigt werden. Die Details, wie diese Risikobewertung schlussendlich zu erfolgen hat, bedarf in diesem Zusammenhang jedoch keiner abschließenden Stellungnahme. Dennoch sollten Herausforderungen der praktischen Umsetzung nicht ausgeblendet werden.<sup>10</sup>

## B. Angemessenheit des Schutzniveaus

### I. Bedeutung der Angemessenheit

Das Schutzniveau und damit die Pflicht nach Art. 32 DS-GVO richtet sich aber nicht ausschließlich nach dieser Risikobewertung. Datenverarbeiter haben vielmehr ein, dem Risiko *angemessenes* Schutzniveau zu gewährleisten. Es bedarf insofern einer Form der Abwägung. Der Gesetzgeber verzichtet damit auf einen absoluten Schutz vor dem ermittelten Risiko.<sup>11</sup> Der Grund hierfür könnte in

---

<sup>8</sup> Vgl., ohne direkten Bezug zum personal data breach: Wennemann, DuD 2018, S. 174, 176 f., zur Zuordnung der dort sog. „Gefährdungen“ nach Art. 32 Abs. 2 DS-GVO zu den „Sicherheitsziele[n]“ für „jede Verarbeitungstätigkeit“; Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 11, der von der Ermittlung „typische[r] Schadensszenarien“ spricht. Siehe auch allgemein zur Risikobewertung innerhalb der Datenschutz-Grundverordnung: Bieker, DuD 2018, S. 27, 29 f., der von „Risikoquellen“ spricht; Ritter/Reibach/Lee, ZD 2019, S. 531, 532, die von „Risikoquellen“ und „möglichen schädigenden Ereignissen“ sprechen.

<sup>9</sup> v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 15; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 8, „gesamten Verarbeitungsvorgang“; vgl. Katko/Meyer, Checklisten zur Datenschutz-Grundverordnung, 2. Aufl. 2023, § 9, Rn. 6, „jedem einzelnen Verarbeitungsschritt“; siehe auch Wennemann, DuD 2018, S. 174, 176, „jede Verarbeitungstätigkeit“; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 1, „zu jedem Zeitpunkt des Verarbeitungsprozesses“; ähnlich Jahnel/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 2, „zu jeder Zeit der Verarbeitung“.

<sup>10</sup> Dieser Punkt wird in Teil 4 *Lösungsvorschlag für das Spannungsverhältnis* berücksichtigt.

<sup>11</sup> Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 46; Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO,

den ansonsten bestehenden Problemen der praktischen Umsetzung eines absoluten Schutzes liegen. So dürfte es bereits schwer möglich sein, die Sicherheit der Verarbeitung vollumfänglich zu gewährleisten.<sup>12</sup> Doch selbst wenn man eine absolute Sicherheit für möglich hielte, dürfte sie wohl dann nur mit einem sehr hohen Aufwand durchsetzbar sein.<sup>13</sup> Eine Verpflichtung zur Gewährleistung einer absoluten Sicherheit der Verarbeitung dürfte daher wenigstens dem Gebot

---

Rn. 3; *Schlegel*, ZD 2020, S. 243, 246; vgl. *Plath/Grages*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 2; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 8; BeckOK Datenschutzrecht/*Paulus*, Stand: 46. Ed. 2023, Art. 32 DS-GVO (Stand: November 2021), Rn. 7; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3; *Suwelack*, ZD 2020, S. 561, 565.

<sup>12</sup> *Gola/Heckmann/Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11, wonach „das Risiko nicht völlig ausgeschlossen werden kann“; *Auernhammer/Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 3; *Gierschmann u.a./Jergl*, Datenschutz-Grundverordnung, 2018, Art. 32 DS-GVO, Rn. 40; siehe auch *Simitis/Hornung/Spiecker gen. Döhmann/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 21, die auf ein mögliches „Restrisiko“ abstellt; ähnlich *Kipker/Reusch/Ritter/Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 35; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 8 verweist darauf, dass dies aufgrund der Ermittlung anhand von Wahrscheinlichkeitsprognosen auch nicht möglich sei.

<sup>13</sup> Vgl. *Ehmann/Selmayr/Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 4, der auf den damit steigenden Aufwand verweist; ähnlich *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 8, die dann auf die Unverhältnismäßigkeit verweist; ähnlich *Gierschmann u.a./Jergl*, Datenschutz-Grundverordnung, 2018, Art. 32 DS-GVO, Rn. 40. Siehe auch *Specht-Riemenschneider/Werry/Werry/Schmidt*, Datenrecht in der Digitalisierung, 2020, § 2.1, Rn. 22, zwar nicht konkret zu Art. 32 DS-GVO, sondern allgemein zur „Erfüllung datenschutzrechtlicher Anforderungen“.

der Verhältnismäßigkeit<sup>14</sup> nicht gerecht werden.<sup>15</sup> Das Gebot der Verhältnismäßigkeit dürfte sich in Art. 32 Abs. 1 DS-GVO in der „Angemessenheit“ des Schutzniveaus ausdrücken.<sup>16</sup>

Setzt die Angemessenheit des zu gewährleistenden Schutzniveaus eine Abwägung voraus, so ist zu klären, welche Kriterien für diese Abwägung zu berück-

---

<sup>14</sup> Allgemein zum Grundsatz der Verhältnismäßigkeit im Europäischen Recht: EuGH, verb. Rs. C-41/79, C-121/79, C-796/79 (Testa), ECLI:EU:C:1980:163 = BeckRS 2004, 71137, Rn. 21; EuGH, verb. Rs. C-453/03, C-11/04, C-12/04, C-194/04 (ABNA u.a.), ECLI:EU:C:2005:741 = BeckRS 2005, 70934, Rn. 68; EuGH, Rs. C-58/08 (Vodafone u.a.), ECLI:EU:C:2010:321 = MMR 2010, S. 561, Rn. 51; EuGH, verb. Rs. C-92/09, C-93/09 (Volker und Markus Schecke und Eifert), ECLI:EU:C:2010:662 = EuZW 2010, S. 939, Rn. 74; Calliess/Ruffert/*Calliess*, EUV/AEUV, 6. Aufl. 2022, Art. 5 EUV, Rn. 44 ff.; *Trstenjak/Beysen*, EuR 2012, S. 265 ff.; *von Danwitz*, EWS 2003, S. 393 ff.; *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, 2003.

<sup>15</sup> Das Art. 32 DS-GVO diesem Gebot folgt: Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 29; Spindler/Schuster/*Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 3; Kuner/Bygrave/Docksey/*Burton*, GDPR, 2020, p. 635; Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 9; Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 18; Freund u.a./*Freund/Schöning*, DSGVO, 2023, Art. 32 DS-GVO, Rn. 43; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 9; *Suwelack*, ZD 2020, S. 561, 565; wohl etwas zurückhaltender Auernhammer/*Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 51 f.

<sup>16</sup> Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 18, „Angemessenheit bzw. Verhältnismäßigkeit“; vgl. auch Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10, der jedenfalls auf die Verhältnismäßigkeit im Rahmen des „angemessenen Schutzniveau“ verweist; siehe auch Kuner/Bygrave/Docksey/*Burton*, GDPR, 2020, p. 635, der „appropriateness“ mit dem „principle of proportionality“ verbindet, wobei aber anzumerken ist, dass die englische Fassung den Begriff „appropriate“ in Art. 32 Abs. 1 DS-GVO drei Mal (einmal auch im Zusammenhang des Schutzniveaus („level of security appropriate to the risk“)) verwendet. Andere verweisen wohl im Zusammenhang der „Geeignetheit“ der Maßnahmen auf das Gebot der Verhältnismäßigkeit: Spindler/Schuster/*Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 9. Siehe zur Verbindung dieser beiden Tatbestände: Kap. 5, C., III., 3. Die „Geeignetheit“ als Einschränkung?.

sichtigen sind. Fest steht, dass das Risiko für die Rechte und Freiheiten betroffener Personen ein Kriterium dieser Abwägung sein muss. Schließlich bezieht sich das zu gewährleistende Schutzniveau auf dieses Risiko<sup>17</sup> und bildet den Ausgangspunkt bei dessen Bestimmung. Um dem Gebot der Verhältnismäßigkeit allerdings gerecht werden zu können, muss es aber noch weitere Kriterien geben, die dann (vor allem) als entsprechende „Gegengewichte“ zu dem Risiko für die Rechte und Freiheiten betroffener Personen fungieren könnten.

## II. Bestimmung der Angemessenheit nach Art. 32 Abs. 2 DS-GVO

### 1. Die offenen Aufzählungen des Art. 32 Abs. 2 DS-GVO

Weitere Kriterien für die Bestimmung der Angemessenheit könnten zunächst in Art. 32 Abs. 2 DS-GVO zu finden sein. Nach dem Wortlaut widmet sich dieser explizit der Beurteilung des angemessenen Schutzniveaus.<sup>18</sup> Konkret zählt Art. 32 Abs. 2 DS-GVO allerdings nur – unter der missverständlichen Bezeichnung –<sup>19</sup> die „Risiken, die mit der Verarbeitung verbunden sind“<sup>20</sup> auf, die bei der Bestimmung des angemessenen Schutzniveaus zu berücksichtigen sind. Wie bereits in dem allgemeinen Teil zu den Zielen des Art. 32 DS-GVO herausgearbeitet wurde, handelt es sich hierbei um Sicherheitsvorfälle, die eine Gefahr und letztlich ein Risiko für die Rechte und Freiheiten betroffener Personen bei der Verarbeitung ihrer Daten darstellen können.<sup>21</sup> Als Teil des Risikos für die Rechte und Freiheiten sind sie damit bereits notwendigerweise auch Teil der Angemessenheitsprüfung. Sie sind aber kein gesondertes Kriterium, das es gilt, im Rahmen der Angemessenheit, mit dem Risiko abzuwägen. An dieser Stelle treten erneut die regelungstechnischen Probleme des Art. 32 DS-GVO hervor, auf die bereits hingewiesen wurde.<sup>22</sup>

Andere Kriterien, die bei der Angemessenheit berücksichtigt werden könnten, beschreibt Art. 32 Abs. 2 DS-GVO hingegen nicht. Auffällig ist jedoch die

<sup>17</sup> Siehe hierzu: Kap. 4, B., II. *Risiko für die Rechte und Freiheiten (natürlicher) Personen.*

<sup>18</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO.*

<sup>19</sup> Zu dieser Kritik: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO.*

<sup>20</sup> Englisch: „risks that are presented by processing“, Französisch: „risques que présente le traitement“, Spanisch: „los riesgos que presente el tratamiento de datos“, Italienisch: „dei rischi presentati dal trattamento“, Niederländisch: „verwerkingsrisico’s“.

<sup>21</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO.*

<sup>22</sup> Hierzu ausführlicher: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO.*



nicht abschließende Aufzählung der Kriterien für die Bestimmung des angemessenen Schutzniveaus in Art. 32 Abs. 2 DS-GVO. Hiermit ist jedoch nicht die offene Aufzählung der, mit der Verarbeitung verbundenen, Risiken gemeint. Diese offene Aufzählung wurde ebenfalls zuvor behandelt und (rechtspolitisch) kritisiert, da es hiermit zu einer Abweichung von dem Begriff des personal data breach nach Art. 4 Nr. 12 DS-GVO kommt.<sup>23</sup> Gemeint ist vielmehr die offene Aufzählung zuvor.

Denn Art. 32 Abs. 2 DS-GVO enthält – ausgehend vom Wortlaut – zwei nicht abschließende Aufzählungen. So heißt es in Art. 32 Abs. 2 DS-GVO:

„Bei der Beurteilung des angemessenen Schutzniveaus sind *insbesondere* [Anm. d. Verf.: Beginn der ersten, nicht abschließenden Aufzählung] die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, *insbesondere* [Anm. d. Verf.: Beginn der zweiten, nicht abschließenden Aufzählung] durch [...]“<sup>24</sup>.

Während also das zweite „*insbesondere*“ sich auf die „Risiken, die mit der Verarbeitung verbunden sind“ bezieht, knüpft das erste „*insbesondere*“ an die Beurteilung des angemessenen Schutzniveaus insgesamt an. Die „Risiken, die mit der Verarbeitung verbunden sind“, wären damit nur ein Teil der Bestimmung des angemessenen Schutzniveaus. Daher müssten auch noch weitere Kriterien bestehen. Welche dies jedoch sein könnten, bleibt zunächst unklar. In der Litera-

<sup>23</sup> Siehe hierzu: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle*.

<sup>24</sup> Hervorhebung durch Verfasser. Nachfolgend die Auszüge aus den anderen Sprachfassungen mit entsprechender Hervorhebung der relevanten Stellen durch Verf. Englisch: „In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from [...]“, Französisch: „Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment [...]“, Spanisch: „Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia [...]“, Italienisch: „Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare [...]“, Niederländisch: „Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg [...]“.

tur fehlt es hierzu meist schon an einer klaren Unterscheidung zwischen den beiden Aufzählungen.<sup>25</sup> Welche weiteren Kriterien von der ersten Aufzählung umfasst sein sollen, wird nicht ausdrücklich benannt.

## 2. Hinweise zur Konkretisierung der Aufzählungen in den Erwägungsgründen

Im Zusammenhang mit dem Risiko für die Rechte und Freiheiten und damit auch dem darauf gerichteten Schutzniveau wird zudem auf den ErwG 75 DS-GVO abgestellt.<sup>26</sup> Daher könnten dort Hinweise zu finden sein, welche weiteren Kriterien bei der Beurteilung des angemessenen Schutzniveaus zu berücksichtigen sind und ggf. von der ersten Aufzählung umfasst sein könnten. Zunächst verweist ErwG 75 DS-GVO darauf, dass Risiken für die Rechte und Freiheiten aus der Verarbeitung hervorgehen können, die zu einem Schaden führen können. Der Schaden kann dabei physischer, materieller oder immaterieller Art sein. Anschließend führt der Erwägungsgrund eine umfassende Liste von Beispielen an. Hierzu gehören u.a. Diskriminierungen, Identitätsdiebstahl oder die unbefugte Aufhebung einer Pseudonymisierung. Ferner stellt der Erwägungsgrund auf die besonderen Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DS-GVO und den strafrechtlichen Daten i.S.d. Art. 10 DS-GVO ab. Weiterhin wird auch auf besondere Verarbeitungsverfahren wie die Persönlichkeitsbewertung verwiesen.

Ob es sich hierbei aber um Kriterien handelt, die die Bewertung der Angemessenheit des Schutzniveaus ergänzen und unmittelbar in den Aufzählungen des Art. 32 Abs. 2 DS-GVO zu berücksichtigen sind, dürfte hingegen fraglich sein. Ähnlich wie die „Risiken, die mit der Verarbeitung verbunden sind“ nach Art. 32 Abs. 2 DS-GVO beziehen sich die Beispiele des ErwG 75 DS-GVO nur

---

<sup>25</sup> Eine Differenzierung nimmt Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 59, „durch das zweite ‚insbesondere‘“ vor; v. Lewinski/Rüpkke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 27, „weiteren ‚insbesondere‘-Aufzählung“; auch Jahnelt/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 13 verweist auf „[d]ie zweimalige Verwendung“.

<sup>26</sup> Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 42 f.; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 30.

auf das Risiko für die Rechte und Freiheiten betroffener Personen. Anders jedoch als die, mit der Verarbeitung verbundenen Risiken, beschreiben sie nicht die Gefahren, die zu einem entsprechenden Risiko für die Rechte und Freiheiten führen, sondern konkretisieren dieses Risiko selbst. Dies lässt sich an einem Beispiel verdeutlichen:

*Der unbefugte Zugang zu personenbezogenen Daten eines Dritten stellt eine Gefahr für die Sicherheit dar, wie sie durch die „Risiken, die mit der Verarbeitung verbunden sind“ nach Art. 32 Abs. 2 DS-GVO beschrieben wird. Diese Gefahr kann zu einem Risiko für die Rechte und Freiheiten betroffener Personen i.S.d. Art. 32 Abs. 1 DS-GVO führen, da der Dritte die unbefugt zugänglichen Daten verwenden kann, um die Identität der betroffenen Person anzunehmen (Identitätsdiebstahl) und ihr damit – bspw. im Fall von Kreditkarteninformationen – einen wirtschaftlichen Schaden zuzufügen.*

Ähnliches gilt für die besondere Hervorhebung von bestimmten Datenkategorien oder Verarbeitungsverfahren. Da hierdurch bspw. bei sensiblen Daten das Risiko für die Rechte und Freiheiten der betroffenen Person höher zu bewerten sein dürfte.<sup>27</sup>

Wie aus dem Einleitungssatz von ErwG 75 DS-GVO bereits hervorgeht, konkretisiert dieser daher nur das Risiko für die Rechte und Freiheiten betroffener Personen, das als Kriterium für die Bestimmung des angemessenen Schutzniveaus bereits umfasst ist. Ein eigenständiges, zusätzliches Kriterium, dass i.S.d. ersten Aufzählung des Art. 32 Abs. 2 DS-GVO bei der Bestimmung des angemessenen Schutzniveaus zu berücksichtigen wäre, findet sich in ErwG 75 DS-GVO hingegen nicht.

### *3. Systematisierung des Art. 32 Abs. 2 DS-GVO*

Damit bleibt aber weiterhin unklar, welche Kriterien bei der Bestimmung des angemessenen Schutzniveaus oder im Zusammenhang der ersten Aufzählung des Art. 32 Abs. 2 DS-GVO zu berücksichtigen sind. Dennoch zeigt die nähere

---

<sup>27</sup> Vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 51; Dat-Komm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 23; Simitis/Horning/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27.

Betrachtung des Art. 32 Abs. 2 DS-GVO einen der Regelung zugrundeliegenden Ansatz, der für die Lösung hilfreich sein kann.

Auch wenn hier das zweite „insbesondere“ und die dazu führende, nicht abschließende Aufzählung im Zusammenhang mit den „Risiken, die mit der Verarbeitung verbunden sind“ kritisiert und eine „Streichung“ mittels einer teleologischen Reduktion befürwortet wird,<sup>28</sup> könnte die Differenzierung der beiden Aufzählungen, wie sie der Wortlaut des Art. 32 Abs. 2 DS-GVO kennt, jedoch von entscheidender Bedeutung sein. Denn die Datenschutz-Grundverordnung ordnet diese Aufzählungen auf verschiedene Ebenen an und lässt damit ein System erahnen, dass weiteren Aufschluss über die erste Aufzählung geben könnte.

Die folgende Abbildung stellt dies einmal grafisch dar:

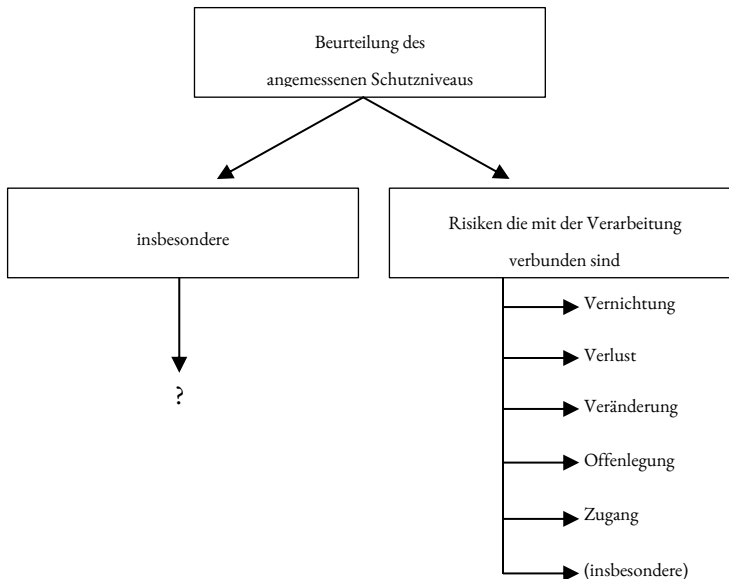


Abb. 2: Ebenen der Aufzählungen des Art. 32 Abs. 2 DS-GVO (eigene Darstellung)

Die Datenschutz-Grundverordnung trägt zu einem großen Teil zu den Auslegungsschwierigkeiten dieser ersten Aufzählung bei. Eine nicht abschließende

<sup>28</sup> Siehe hierzu: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle.*

Aufzählung bildet im Rahmen einer Rechtsvorschrift eine eigene (Unter-)Systematik,<sup>29</sup> wodurch bei ihrer Auslegung die bereits genannten Aufzählungspunkten dabei helfen können, aus ihnen die, von der Aufzählung ebenfalls umfassten, ungenannte Punkte abzuleiten.<sup>30</sup> Art. 32 Abs. 2 DS-GVO benennt mit den „Risiken, die mit der Verarbeitung verbunden sind“ jedoch nur einen einzigen Punkt. Weiterhin ist zu beachten, dass dieser Punkt bei der Bestimmung des angemessenen Schutzniveaus auch noch eine Sonderfunktion einnimmt, indem er eigentlich Teil eines anderen Kriteriums – dem des Risikos für die Rechte und Freiheiten betroffener Personen – ist.<sup>31</sup> Hieraus eine Ableitung für die weiteren, unbenannten Aufzählungspunkte vorzunehmen, ist ohne ergänzende Hinweise unmöglich.

### III. Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?

Auf der Suche nach möglichen Kriterien für die Prüfung der Angemessenheit des Schutzniveaus sticht jedoch erneut Art. 32 Abs. 1 DS-GVO ins Auge. So zählt Art. 32 Abs. 1 DS-GVO gleich zu Beginn mehrere Kriterien auf, die es in irgendeiner Weise zu berücksichtigen gilt. Dies sind namentlich (1) der „Stand

---

<sup>29</sup> Vgl. auch *Schünemann*, JZ 2005, S. 271, 275, „strukturelle Einheit“ zwischen Generalklausel und Regelbeispiel; so auch *Möllers*, Juristische Methodenlehre, 5. Aufl. 2023, § 7, Rn. 22.

<sup>30</sup> Vgl., jedoch nicht speziell zur Europäischen Rechtsmethodik, *Kramer*, Juristische Methodenlehre, 6. Aufl. 2019, S. 314, zur Konkretisierung von Generalklauseln mit zusätzlichem Beispielkatalog, bei denen die Beispiele zur Auslegung der Generalklausel heranzuziehen sind; ähnlich auch *Möllers*, Juristische Methodenlehre, 5. Aufl. 2023, § 7, Rn. 17 ff., wonach Beispiele eine „erhellende Funktion“ für die Wertungen der Generalklausel haben; siehe auch *Schünemann*, JZ 2005, S. 271, 276 f., eingeordnet als „Zurückhaltungsgebot“. Siehe auch zum nationalen Recht bspw. die Auslegung des Begriffs des „sonstigen Rechts“ nach § 823 Abs. 1 BGB, der im Lichte der konkret benannten Rechte des § 823 Abs. 1 BGB auszulegen ist: Vgl. RGZ 57, S. 353, 356, das gerade im Verhältnis zu den vorher genannten Rechtsgütern auf die Gemeinsamkeit des absoluten Rechts abstellt; siehe BGHZ 192, S. 204, Rn. 21 ff., ablehnend zu Domainnamen, da die „Vergleichbarkeit [...] nicht auf einer von der Rechtsordnung eingeräumten Rechtsposition“ (Rn. 24) beruht; *Schulze/A. Staudinger*, BGB, 11. Aufl. 2022, § 823 BGB, Rn. 28; *Jauernig/Kern*, BGB, 19. Aufl. 2023, § 823 BGB, Rn. 12; *BeckOK BGB/Förster*, Stand: 68. Ed. 2023, § 823 BGB (Stand: November 2023), Rn. 143.

<sup>31</sup> Hierzu ausführlicher: Kap. 4, C. Personal data breaches (und andere Sicherheitsvorfälle).

der Technik<sup>32</sup>, (2) die „Implementierungskosten“<sup>33</sup>, (3) verarbeitungsbezogene Kriterien<sup>34</sup> (die sich auflgliedern in: „Art“<sup>35</sup>, „Umfang“<sup>36</sup>, „Umstände“<sup>37</sup> und „Zwecke“<sup>38</sup> der „Verarbeitung“<sup>39</sup>) und (4) die „unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“<sup>40</sup>.

<sup>32</sup> Englisch: „state of the art“, Französisch: „de l'état des connaissances“, Spanisch: „el estado de la técnica“, Italienisch: „dello stato dell'arte“, Niederländisch: „stand van de techniek“.

<sup>33</sup> Englisch: „costs of implementation“, Französisch: „des coûts de mise en œuvre“, Spanisch: „los costes de aplicación“, Italienisch: „dei costi di attuazione“, Niederländisch: „de uitvoeringskosten“.

<sup>34</sup> Ebenfalls für eine Zusammenfassung zu einem (Haupt-)Kriterium: Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 12; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 14. Die niederländische Sprachfassung könnte einer Zusammenfassung der Kriterien entgegenstehen, da sie am Ende vom „Verwendungszweck“ (Niederländisch: „de verwerkingsdoeleinden“) spricht. Sie verwendet damit einen Eigenbegriff, der dann die Frage aufwerfen könnte, ob sich die zuvor genannten Kriterien ebenfalls auf die Verarbeitung beziehen sollen. Aufgrund der anderen – ähnlich zur deutschen – Sprachfassungen und dem Fehlen eines anderen denkbaren Bezugspunkts als die Verarbeitung, dürfte eine Zusammenfassung der Kriterien dennoch gerechtfertigt bleiben.

<sup>35</sup> Englisch: „the nature“, Französisch: „de la nature“, Spanisch: „la naturaleza“, Italienisch: „della natura“, Niederländisch: „de aard“.

<sup>36</sup> Englisch: „scope“, Französisch: „de la portée“, Spanisch: „el alcance“, Italienisch: „dell'oggetto“, Niederländisch: „de omvang“.

<sup>37</sup> Englisch: „context“, Französisch: „du contexte“, Spanisch: „el contexto“, Italienisch: „del contesto“, Niederländisch: „de context“.

<sup>38</sup> Englisch: „purposes“, Französisch: „des finalités“, Spanisch: „los fines“, Italienisch: „delle finalità“, Niederländisch: „de verwerkingsdoeleinden“, wobei die niederländische Sprachfassung für „die Zwecke der Verarbeitung“ einen zusammengesetzten Begriff aus „Zweck“ und „Verarbeitung“ – wie „Verarbeitungszweck“ – verwendet.

<sup>39</sup> Englisch: „processing“, Französisch: „du traitement“, Spanisch: „del tratamiento“, Italienisch: „del trattamento“, Niederländisch: „de verwerkingsdoeleinden“, als zusammengesetzter Begriff, siehe auch die vorangegangene Fußnote.

<sup>40</sup> Nach hier vertretener Ansicht geht es in Bezug auf das Regelungsziel um das Risiko für die betroffenen Personen, vgl. Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*. Siehe aber auch später für die Frage einer Differenzierung: Kap. 7, B., IV., 2. *Möglichkeit einer Doppelfunktion*.

<sup>41</sup> Englisch: „risk of varying likelihood and severity for the rights and freedoms of natural persons“, Französisch: „des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques“, Spanisch: „riesgos de probabilidad y gravedad variables para los

### 1. Problem des Bezugspunkts der Kriterien

Fraglich ist zunächst, ob diese Kriterien sich auch wirklich auf die Angemessenheit des Schutzniveaus beziehen oder einen anderen Bezugspunkt haben. Für Ersteres spricht zunächst, dass auch das „*Risiko für die Rechte und Freiheiten natürlicher*“ [Anm. d. Verf.: wohl eher „betroffener“] *Personen*“ enthalten ist, auf dass das angemessene Schutzniveau verweist<sup>42</sup> und das den Ausgangspunkt für die Prüfung des geforderten Schutzniveaus markiert.<sup>43</sup> Die weiteren Kriterien könnten dann die Faktoren sein, die es gilt, mit dem Risiko abzuwägen. Betrachtet man die weiteren Kriterien nach Art. 32 Abs. 1 Hs. 1 DS-GVO, so fallen gerade die Implementierungskosten auf. Hierbei handelt es sich wohl um ein Kriterium, das den wirtschaftlichen Aufwand zur Gewährleistung der Sicherheit berücksichtigen soll,<sup>44</sup> und damit als ein potenzielles „Gegengewicht“ im Rahmen der Verhältnismäßigkeit dienen könnte.<sup>45</sup>

Aus den Ausführungen in der Diskussion geht hingegen nicht immer deutlich hervor, worauf sich diese Abwägungskriterien des Art. 32 Abs. 1 Hs. 1 DS-GVO beziehen sollen. Bei strenger Betrachtung ließen sich jedenfalls zwei Bezugspunkte festmachen. So könnten sich die Kriterien einmal auf die Auswahl

---

*derechos y libertades de las personas físicas*“, Italienisch: „*del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*“, Niederländisch: „*de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen*“. Der potenziell missverständliche Verweis auf die „*unterschiedliche Eintrittswahrscheinlichkeit*“ und „*Schwere*“ nach Art. 32 Abs. 1 DS-GVO wurde ebenfalls bereits oben thematisiert, Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO*.

<sup>42</sup> Siehe oben: Kap. 4, B., II. *Risiko für die Rechte und Freiheiten (natürlicher) Personen* i.V.m. Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>43</sup> Siehe oben: Kap. 5, A. *Risikobewertung*.

<sup>44</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 11; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 26. Siehe hierzu ausführlicher: Kap. 7, B., II. *Implementierungskosten*.

<sup>45</sup> Statt vieler zunächst: Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 6, der u.a. die Implementierungskosten als „*Korrektiv*“ und „*Grenze*“ beschreibt; siehe ausführlicher zum Kriterium „*Implementierungskosten*“: Kap. 7, B., II. *Implementierungskosten*.

der technischen und organisatorischen Maßnahmen beziehen, die es anschließend<sup>46</sup> zu treffen gilt, um das angemessene Schutzniveau zu gewährleisten.<sup>47</sup> Die Kriterien könnten aber auch früher anzusetzen sein und könnten sich bereits auf die Bestimmung des angemessenen Schutzniveaus beziehen.<sup>48</sup> Anzumerken ist hierbei allerdings, dass die in Frage stehenden Bezugspunkte nicht immer klar voneinander getrennt werden und eine solche Trennung in der praktischen Anwendung der Vorschrift wohl auch nicht immer möglich ist.<sup>49</sup> Daher ist die hier vorgenommene Zuordnung der Stimmen mit Vorsicht zu behandeln. Vorrangiges Ziel dieser Einordnung ist vor allem, das Erfordernis einer gedanklich klaren Differenzierung dieser beiden Punkte zu verdeutlichen.

Denn in den rechtlichen Auswirkungen könnte es einen entscheidenden Unterschied machen, ob sich die Kriterien nach Art. 32 Abs. 1 DS-GVO nun auf die Implementierung der Maßnahmen oder auf das vorausgehende Schutzniveau beziehen. Bei einer strengen Beachtung der Systematik würde eine Abwägung auf nachgelagerter Ebene – also im Rahmen der zu treffenden Maßnahmen – an der grundsätzlichen Verpflichtung, ein angemessenes Schutzniveau

<sup>46</sup> Siehe hierzu ausführlicher: Kap. 5, C., I. *Allgemeines*.

<sup>47</sup> In diese Richtung könnten die folgenden Stimmen verstanden werden: Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 7 ff., die diese Kriterien als „*Auswahlkriterien*“ der Maßnahmen bezeichnet; Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, Art. 32 DS-GVO, Rn. 20 ff., als Einordnung von Abwägungskriterien für die Maßnahmen; Taeger/Gabel *Schultze-Melling*, DS-GVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 13 f., als „*Aspekte bei der Auswahl und Durchführung der Maßnahmen*“.

<sup>48</sup> In diese Richtung könnten die folgenden Stimmen verstanden werden: Schuster/Grütz-macher/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 18; DatKomm/*Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 20 ff., Kriterien für die „*Erreichung eines dem Risiko angemessenen Schutzniveaus*“; Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 20; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 47 f., der diese unter „*dem Risiko angemessenes Schutzniveau*“ behandelt; ähnlich wohl Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10, der diese zwar unter dem Oberpunkt „*Maßnahmen*“ aber in dessen Rahmen unter „*Kriterien der Abwägung, angemessenes Schutzniveau*“ behandelt; Ehmann/Selmayr/*Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 4 f., 11, der die Kriterien in den Kontext der Angemessenheitsprüfung setzt; ähnlich Gärtner/*Selzer*, DuD 2023, S. 289, 290.

<sup>49</sup> Siehe zum Problem der klaren Trennung auch den späteren Lösungsvorschlag: Kap. 12, E. *Ableitung des angemessenen Schutzniveaus*.



zu gewährleisten, nichts ändern. Art. 32 Abs. 1 DS-GVO würde den Verpflichteten zwar bei der Auswahl der zu treffenden Maßnahmen eine Abwägung zugestehen. Es bliebe aber weiterhin dabei, ein – wie dann auch immer zu bestimmendes – angemessenes Schutzniveau zu gewährleisten. Bezieht sich die Abwägung hingegen auf die Angemessenheit des Schutzniveaus selbst, so hätte dies unmittelbare Auswirkungen auf den Pflichtenumfang der Vorschrift. Der Frage des Bezugspunkts der Abwägungsformel kommt damit eine entscheidende Bedeutung bei der weiteren Prüfung des Art. 32 Abs. 1 DS-GVO zu und bedarf daher der Klärung.

## 2. Wortlaut

Der Grund für die (vermeintlich) divergierende und teilweise unklare Einordnung dieser Abwägungskriterien könnte in der Formulierung des Art. 32 Abs. 1 DS-GVO liegen. Dort heißt es, dass:

„Unter Berücksichtigung [der Kriterien], treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, [...]“<sup>50</sup>.

Zunächst scheint es, dass der Wortlaut die erste Ansicht unterstützt und hier „Auswahlkriterien“ für technische und organisatorische Maßnahmen sieht. Art. 32 Abs. 1 Hs. 1 DS-GVO führt aber dann weiter aus:

„[...] um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“<sup>51</sup>.

---

<sup>50</sup> Englisch: „Taking into account [...] the controller and the processor shall implement appropriate technical and organisational measures [...]“, Französisch: „Compte tenu [...] le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées [...]“, Spanisch: „Teniendo en cuenta [...] el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas [...]“, Italienisch: „Tenendo conto [...] il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate [...]“, Niederländisch: „Rekening houdend met [...] treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen [...]“.

<sup>51</sup> Englisch: „[...] to ensure a level of security appropriate to the risk [...]“, Französisch: „[...] afin de garantir un niveau de sécurité adapté au risque [...]“, Spanisch: „[...] para garantizar un nivel de seguridad adecuado al riesgo [...]“, Italienisch: „[...] per garantire un livello di sicurezza adeguato al rischio [...]“, Niederländisch: „[...] om een op het risico afgestemd beveiligingsniveau te waarborgen [...]“.

Der zweite Teil des Satzes könnte hingegen für die zweite Auslegung sprechen, sodass die Kriterien im Zusammenhang mit der Angemessenheit des Schutzniveaus zu berücksichtigen sind. Der Wortlaut lässt mithin beide Interpretationen zu.

### 3. Historische Auslegung

Anhaltspunkte zum Bezugspunkt der Abwägungskriterien könnten sich schließlich auch aus der historischen Entwicklung der Vorschrift und unter Berücksichtigung der zuvor geltenden Datenschutzrichtlinie ergeben. Der Vergleich einer Vorschrift mit ihrer (historischen) Vorgängerregelung zum Zwecke der Auslegung lässt sich nach der europäischen Methodik berücksichtigen.<sup>52</sup>

In Art. 17 Abs. 1 UAbs. 2 DS-RL, als Vorgängerregelung des Art. 32 DSGVO, hieß es noch:

*„Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“<sup>53</sup>*

<sup>52</sup> Allgemein zur Beachtung der Entwicklung durch Vorgängerregelungen bei der Auslegung: EuGH, Rs. C-15/60 (Simon/Gerichtshof), ECLI:EU:C:1961:11 = BeckRS 2004, 71721, S. 260 ff.; EuGH, Rs. C-83/78 (Redmond), ECLI:EU:C:1978:214 = BeckRS 2004, 73798, Rn. 53/54; EuGH, Rs. C-324/14 (Partner Apelski Dariusz), ECLI:EU:C:2016:214 = NZBau 2016, S. 373, Rn. 91; EuGH, verb. Rs. C-164/21, C-318/21 (BALTIJAS STARPTAUTISKĀ AKADĒMIJA), ECLI:EU:C:2022:785 = BeckRS 2022, 27275, Rn. 62 (bzw. Rn. 59 bei BeckRS). Siehe auch in der Literatur: *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 255 ff.; *Henninger*, Europäisches Privatrecht und Methode, 2009, S. 288; *Müller/Christensen*, Juristische Methodik, II. Bd. Europarecht, 3. Aufl. 2012, Rn. 71; *Lutter*, JZ 1992, S. 593, 599 f.

<sup>53</sup> Englisch: *„Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.“*, Französisch: *„Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.“*, Spanisch: *„Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.“*, Italienisch: *„Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.“*, Niederländisch: *„Deze maatregelen moeten, rekening houdend met de stand van de techniek en*

Die Datenschutzrichtlinie sah damit auch in Art. 17 Abs. 1 UAbs. 2 DS-RL eine Angemessenheitsabwägung vor.<sup>54</sup> Wie die Verordnung, stellt die Datenschutzrichtlinie zwar ebenfalls sowohl auf die (technischen und organisatorischen) Maßnahmen als auch auf das Schutzniveau ab. Im Gegensatz zur Formulierung in der Datenschutz-Grundverordnung bezieht die Richtlinie die – mit Art. 32 Abs. 1 Hs. 1 DS-GVO vergleichbaren – Kriterien aber deutlicher auf die Angemessenheit des Schutzniveaus und weniger auf die zu treffenden Maßnahmen.

Dies wird besonders deutlich durch die Trennung von der Pflicht zur Implementierung entsprechender Maßnahmen (Art. 17 Abs. 1 UAbs. 1 DS-RL) und den Anforderungen daran, mit diesen Maßnahmen ein angemessenes Schutzniveau zu erreichen (Art. 17 Abs. 1 UAbs. 2 DS-RL). Die Datenschutz-Grundverordnung versucht hingegen beide Punkte in einem Satz zu behandeln. Trotz der sprachlichen Änderungen finden sich im Gesetzgebungsprozess aber auch keine Hinweise darauf, dass die Datenschutz-Grundverordnung von diesem generellen System, welches so bereits unter der Datenschutzrichtlinie galt, abweichen wollte.<sup>55</sup> Dies lässt sich bereits daran erkennen, dass sich zwar der Verordnungstext in seiner Formulierung verändert hat, eine mit Art. 17 Abs. 1 UAbs. 2 DS-

---

*de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen.“*

<sup>54</sup> Vgl. Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 9, mit dem Verweis auf eine „*Verhältnismäßigkeitsprüfung*“; auch Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10, jedoch mit Verweis auf die deutsche Umsetzung in § 9 BDSG a.F.; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 26, mit Verweis auf „*in der Tradition des Art. 17 DSRL*“ und einer dort ebenfalls vorzunehmenden „*Güterabwägung*“.

<sup>55</sup> Vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 3, die in den Änderungen zur Vorgängerregelung mehr eine Konkretisierung sieht; ähnlich Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 21 ff.; wohl auch Spiecker gen. Döhmann u.a./Papadaki/Stalla-Bourdillon, GDPR, 2023, Art. 32 GDPR, Rn. 1, 9; siehe auch Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 1, der im Vergleich zu Art. 17 DS-RL herausstellt, dass nun auch Auftragsverarbeiter verpflichtet sind; so auch Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 1. A.A. wohl Sander, PinG 2017, S. 250, 252 f, der in Art. 32 DS-GVO eine Abkehr von der bisherigen Rechtslage des § 9 BDSG a.F. bzw. Art. 17 DS-RL sieht; siehe auch Feiler/Forgó, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 32 DS-GVO, Rn. 8, die ebenfalls Unterschiede zu Art. 17 DS-RL sehen.

RL vergleichbare Formulierung findet sich allerdings noch in Erwägungsgrund 83 S. 2 DS-GVO wieder.

#### 4. Systematik und Telos

Erkenntnisse aus der Systematik der Vorschrift und ihrem Telos lassen sich in diesem Fall nur schwer voneinander trennen, da sie hier stark miteinander verflochten sind.<sup>56</sup> Entscheidend ist hier vor allem, dass die Verordnung mit dem angemessenen Schutzniveau erkennbar keinen absoluten Maßstab zugrunde legt und vielmehr eine Berücksichtigung der Umstände verlangt.<sup>57</sup> Damit bedarf es aber auch zwingend entsprechender Kriterien, die bei einer hierfür erforderlichen Abwägung berücksichtigt werden sollen.

Wie bereits zuvor dargestellt, liefert Art. 32 DS-GVO keine anderen Kriterien, die man im Rahmen einer solchen Abwägung berücksichtigen könnte. Gerade der Art. 32 Abs. 2 DS-GVO, der sich zwar vorrangig der Bestimmung des angemessenen Schutzniveaus widmen möchte, hilft hier nicht weiter.<sup>58</sup> Die dort einzig klar benannten Kriterien fließen bereits im Rahmen der Risikobewertung in diese Abwägung ein. Andere denkbare Kriterien sind hinter einer offenen Aufzählung versteckt. Ohne nähere Anhaltspunkte, welche weiteren Kriterien der Gesetzgeber von dieser Aufzählung umfasst wissen möchte, lässt sich diese aber auch nicht interpretieren.

Fast schon im Wege eines „Ausschlussverfahrens“ bleiben somit nur noch die Kriterien nach Art. 32 Abs. 1 Hs. 1 DS-GVO übrig. Und betrachtet man diese inhaltlich, so liegt die Anwendung im Rahmen der Angemessenheitsprü-

---

<sup>56</sup> Siehe zur engen Verbindung beider Auslegungsmethoden: *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 200 ff.; *Herresthal*, ZEuP 2009, S. 598, 606; *Henninger*, Europäisches Privatrecht und Methode, 2009, S. 283; *Adrian*, Grundprobleme einer juristischen (gemeinschaftsrechtlichen) Methodenlehre, 2009, S. 422; *Colneric*, ZEuP 2005, S. 225, 227, wonach beide Auslegungsformen „*untrennbar ineinander übergeben*“. Erklären ließe sich diese Verbindung damit, wenn man, wie einige Stimmen vertreten, die teleologische Auslegung als Methodenform ablehnt und den Telos vielmehr nur als Ziel der Auslegung ansieht, das durch die anderen Auslegungsformen zu bestimmen ist. Siehe zu dieser Ansicht: *Höpfner/Rüthers*, AcP 209 (2009), S. 1, 7 f.; *Müller*, „*Babylonische Sprachverwirrung*“, in: FS Mayer, 2011, S. 391, 400; *Rüthers/Fischer/Birk*, Rechtslehre, 12. Aufl. 2022, Rn. 725 ff.

<sup>57</sup> Siehe hierzu bereits: Kap. 5, B., I. *Bedeutung der Angemessenheit*.

<sup>58</sup> Siehe hierzu: Kap. 5, B., II. *Bestimmung der Angemessenheit nach Art. 32 Abs. 2 DS-GVO*.

fung nahe. Denn die Verordnung benennt hier erstmals Kriterien, die im Rahmen der Abwägung als „Gegengewicht“ fungieren könnten und damit dem Gebot der Verhältnismäßigkeit – was die Verordnung mit dem angemessenen Schutzniveau zugrunde legt –<sup>59</sup> gerecht werden könnte.

### *5. Eigene Lösung*

Unter Berücksichtigung der Erkenntnisse aus den verschiedenen Auslegungsmethoden können sich die Kriterien nach Art. 32 Abs. 1 Hs. 1 DS-GVO nur auf die Abwägung im Rahmen der Angemessenheit des Schutzniveaus beziehen. Ein Bezug alleine auf die Auswahl der zu treffenden Maßnahmen würde hingegen keinen Sinn ergeben, wenn sich hierdurch nichts an dem Pflichtenumfang der Vorschrift ändert.

Aus den oben beschriebenen Gründen ist eine solche Differenzierung zwischen der Verpflichtung ein angemessenes Schutzniveau zu gewährleisten und dessen Umsetzung durch technische und organisatorische Maßnahmen für das Regelungsverständnis des Art. 32 DS-GVO zwingend geboten. Daher sollten die Abwägungskriterien des Art. 32 Abs. 1 Hs. 1 DS-GVO auch klar der Ebene der Angemessenheit des Schutzniveaus zugeordnet werden.

### *IV. Zwischenergebnis*

Die Angemessenheit des Schutzniveaus setzt eine Abwägung voraus. Art. 32 DS-GVO verzichtet insofern auf einen absoluten Schutz und folgt damit dem Grundsatz der Verhältnismäßigkeit. Teil dieser Abwägung ist einmal die zuvor erfolgte Risikobewertung, woran das Schutzniveau erstmalig auszurichten ist.

Die weiteren Abwägungskriterien sind in Art. 32 DS-GVO etwas versteckt. Zwar knüpft Art. 32 Abs. 2 DS-GVO vorrangig an das angemessene Schutzniveau sowie dessen Bestimmung an und lässt darauf schließen, dass auch entsprechende Kriterien hierfür definiert werden. Außer den dort definierten Gefahren für das Risiko für die Rechte und Freiheiten betroffener Personen hilft Absatz 2 nur wenig weiter, da die weiteren Kriterien zur Bestimmung des angemessenen Schutzniveaus hinter einer offenen Aufzählung unbenannt bleiben.

Dagegen kennt aber auch Art. 32 Abs. 1 Hs. 1 DS-GVO Kriterien, die sich – nach Auslegung – als Abwägungskriterien zur Bestimmung der Angemessenheit des Schutzniveaus herausstellen. Neben dem Risiko für die Rechte und

---

<sup>59</sup> Siehe hierzu: Kap. 5, B., I. *Bedeutung der Angemessenheit*.

Freiheiten betroffener Personen handelt es sich bei diesen um den Stand der Technik, die Implementierungskosten und entsprechende verarbeitungsbezogene Kriterien, die es zu beachten gilt.

## C. Technische und organisatorische Maßnahmen

### I. Allgemeines

Die Gewährleistung des angemessenen Schutzniveaus erfolgt anschließend mittels geeigneter technischer und organisatorischer Maßnahmen. Eine Definition, was der Gesetzgeber unter technischen und organisatorischen Maßnahmen verstehen möchte, findet sich in der Datenschutz-Grundverordnung hingegen nicht.<sup>60</sup> Nicht nur im Zusammenhang mit der Sicherheit der Verarbeitung nach Art. 32 Abs. 1 DS-GVO bedient sich die Datenschutz-Grundverordnung dieses Begriffs.<sup>61</sup> So stellen insb. auch die Art. 24, 25 DS-GVO auf die technischen und organisatorischen Maßnahmen ab.

Was bei der Anknüpfung an die technischen und organisatorischen Maßnahmen zunächst auffällt, sind ihre verschiedenen Wirkungsweisen. Im Falle des Art. 32 Abs. 1 DS-GVO stellt die Schaffung eines angemessenen Schutzniveaus das rechtlich „gewünschten“ Ziel dar, das Datenverarbeiter zu gewährleisten haben. Die technischen und organisatorischen Maßnahmen sollen dieses rechtlich gewünschte Ziel auf tatsächlicher Ebene gewährleisten. Im Zusammenhang mit anderen Vorschriften kann den technischen und organisatori-

---

<sup>60</sup> v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 17; Roßnagel/Husemann, Das neue Datenschutzrecht, 2018, § 5, Rn. 152. Zum wortgleichen Begriff in Art. 24 DS-GVO: Taeger/Gabel/Lang, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 24 DS-GVO, Rn. 23; Kühling/Buchner/Hartung, DS-GVO – BDSG, 4. Aufl. 2024, Art. 24 DS-GVO, Rn. 17.

<sup>61</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 28; Taeger/Gabel/Lang, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 24 DS-GVO, Rn. 23; Kühling/Buchner/Hartung, DS-GVO – BDSG, 4. Aufl. 2024, Art. 24 DS-GVO, Rn. 17; v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 8.

schen Maßnahmen eine andere Funktion als die Sicherheit der Verarbeitung zukommen.<sup>62</sup> Sie dienen damit lediglich als Werkzeug zur Umsetzung der jeweiligen Vorschriften.

Dabei ist der Begriff der „*Maßnahmen*“<sup>63</sup> von seinem Wortlaut nach sehr weit.<sup>64</sup> In Verbindung mit dem Ziel eines, für das Risiko angemessenen Schutzniveaus dürfte darunter jedes Mittel fallen, das in der Lage ist, einen Beitrag zur Gewährleistung des geforderten Schutzniveaus zu leisten.<sup>65</sup>

Von besonderer Bedeutung für den Konflikt bei datenverarbeitenden TOM ist dabei die Frage, ob die Datenschutz-Grundverordnung zwingende Vorgaben an die Maßnahmen stellt, wie bspw. die Pflicht zur Implementierung bestimmter TOM. Gesetzliche Vorgaben an die Implementierung stellen für eine Lösung des Problems einen wichtigen Faktor dar. Der eigentlich sehr weite Begriff der „*Maßnahmen*“ könnte damit durch Art. 32 DS-GVO weiter eingegrenzt werden. Nach Art. 32 DS-GVO kommen hier drei Aspekte in Betracht, aus denen sich gesetzliche Vorgaben an die Maßnahmen ergeben könnten.

---

<sup>62</sup> Vgl. statt vieler: Roßnagel/Husemann, Das neue Datenschutzrecht, 2018, § 5, Rn. 134, 152; siehe hierzu bereits: Kap. 2, C., I. *Das Spannungsverhältnis bei datenverarbeitenden TOM in der aktuellen Diskussion*.

<sup>63</sup> Englisch: „*measures*“, Französisch: „*les mesures*“, Spanisch: „*medidas*“, Italienisch: „*misure*“, Niederländisch: „*maatregelen*“.

<sup>64</sup> Vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 28, „*alle Handlungen*“, vgl. auch dort die Kommentierung zu Art. 24 DS-GVO, Rn. 20a. In Bezug auf eine weite Auslegung des gesamten Begriffs „*technische und organisatorische Maßnahmen*“: v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 8; Roßnagel/Husemann, Das neue Datenschutzrecht, 2018, § 5, Rn. 152; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 12.

<sup>65</sup> Vgl. Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 12; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 28, siehe zudem dort seine Kommentierung des Art. 24, Rn. 20a; vgl. auch BeckOK Datenschutzrecht/Schmidt/Brink, Stand: 46. Ed. 2023, Art. 24 DS-GVO (Stand: November 2023), Rn. 12, zum wortgleichen Begriff in Art. 24 DS-GVO mit dem Verweis „*dem Ziel [zu] dienen*“; siehe auch Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 36, wobei sie dies wohl eher an dem Tatbestand „*geeignet*“ festmachen möchten (hierzu noch sogleich: Kap. 5, C., III. *Geeignetheit der Maßnahmen*).

## II. Technischer und organisatorischer Art

Die Maßnahmen müssen zunächst einmal technischer oder organisatorischer Art sein. Hieraus könnten sich gleich zwei nennenswerte Einschränkungen – und damit Vorgaben – an die Maßnahmen ergeben. Die Konkretisierung auf die Art der Maßnahmen könnte als Ausdruck verstanden werden, dass es für Art. 32 Abs. 1 DS-GVO wohl nicht unerheblich ist, um welche Maßnahmen es sich handelt, die die Sicherheit der Verarbeitung gewährleisten sollen.

Technische Maßnahmen greifen dabei auf eine technische Funktionsweise zurück.<sup>66</sup> Sie zielen auf die Verarbeitung selbst ab.<sup>67</sup> Solche Maßnahmen könnten bspw. in einem Passwortschutz für einen Datenzugriff liegen.<sup>68</sup> Aber auch einfache, bauliche Maßnahmen, wie Brandschutztüren<sup>69</sup>, die vor der Zerstörung von Datenbeständen durch Brände sichern, können hierunter zu verstehen sein.<sup>70</sup>

---

<sup>66</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 24 DS-GVO, Rn. 21, siehe auch dort seine Kommentierung des Art. 32 DS-GVO, Rn. 28, mit Verweis auf Art. 24 DS-GVO; vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 5; v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 17.

<sup>67</sup> Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 37; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 5; Gärtner/Selzer, DuD 2023, S. 289, 290; siehe auch Taeger/Gabel/Lang, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 24 DS-GVO, Rn. 24, zu Art. 24 DS-GVO.

<sup>68</sup> Vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 24 DS-GVO, Rn. 21, zwar als Beispiel für Art. 24 DS-GVO, doch ein Passwortschutz kann auch eine technische Maßnahme für Art. 32 DS-GVO darstellen.

<sup>69</sup> Vgl. auch Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 19, „Brandschutzmaßnahmen“; siehe auch Schuster/Grützmacher/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 84, unter „Besondere technische Maßnahmen für Serverräume/Rechenzentren“ den Punkt „baulicher Brandschutz“. Siehe allgemein zu Brandschutzmaßnahmen als TOM Schläger/Thode/Schirrmacher, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel I, Rn. 198 ff.

<sup>70</sup> Allgemein zu Erfassung baulicher Maßnahmen: Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 26; Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 18; siehe auch Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 24 DS-GVO, Rn. 21, zu Art. 24 DS-GVO.



Organisatorische Maßnahmen zielen auf die „äußeren Rahmenbedingungen“<sup>71</sup> der Verarbeitung.<sup>72</sup> Ein Beispiel für organisatorische Maßnahmen könnten Verhaltensregeln für die Herausgabe gespeicherter Daten sein, um sicherzustellen, dass die anfragende Person berechtigt ist, diese Daten zu erhalten.<sup>73</sup> Der Begriff der organisatorischen Maßnahmen ist daher sehr weit zu verstehen und umfasst auch rechtliche Maßnahmen.<sup>74</sup>

Eine wirkliche Einschränkung auf bestimmte Maßnahmen ergibt sich dadurch freilich nicht. Der Umfang denkbarer Maßnahmen bleibt weiterhin sehr weit.<sup>75</sup>

Eine weitere Frage, die sich im Zusammenhang technischer und organisatorischer Maßnahmen stellt, ist, ob der Gesetzgeber zwingend sowohl technische als auch organisatorische Maßnahmen verlangt. Handelt es sich insofern bei dem „und“ um eine kumulative Voraussetzung, was zur Folge hätte, dass zwingend technische wie auch organisatorische Maßnahmen getroffen werden müssen? Der Gesetzgeber könnte mit dem „und“ aber auch schlicht ausdrücken wollen, dass es sowohl technische als auch organisatorische Maßnahmen gibt, derer man sich bedienen kann, ohne hiermit eine Pflicht aufzuerlegen, beide Maßnahmenarten gleichzeitig einzusetzen.

---

<sup>71</sup> Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 24 DS-GVO, Rn. 22 und den Verweis in Art. 32 DS-GVO, Rn. 28 auf die Kommentierung von Art. 24 DS-GVO.

<sup>72</sup> Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 24 DS-GVO, Rn. 22 und den Verweis in Art. 32 DS-GVO, Rn. 28 auf die Kommentierung von Art. 24 DS-GVO; Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 37; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 5; *Gärtner/Selzer*, DuD 2023, S. 289, 290.

<sup>73</sup> Ähnliche Beispiele bei *v. Lewinski/Rüpkke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 17, „Arbeitsanweisungen, Richtlinien, Dokumentations- und Berichtspflichten“ und „Kontrollen“; Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 37, „interne Handlungsanweisungen“; Auernhammer/*Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 67, „Anweisungen zur Passwortqualität und Änderungszyklen“.

<sup>74</sup> Siehe *v. Lewinski/Rüpkke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 17, wonach unter die organisatorischen Maßnahmen alle Maßnahmen fallen, die nicht technisch sind.

<sup>75</sup> Siehe für ein weites Verständnis: *v. Lewinski/Rüpkke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 8; Roßnagel/*Husemann*, Das neue Datenschutzrecht, 2018, § 5, Rn. 152; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 12.

Eine praktische Relevanz wird dem Ergebnis dieser Frage wohl nicht zukommen, denn die Grenzen zwischen technischen und organisatorischen Maßnahmen können nicht immer scharf gezogen werden.<sup>76</sup> So werden bspw. in Unternehmensrichtlinien häufig Anforderungen an die Qualität von Passwörtern vorgeschrieben (bspw. eine Mindestzeichenlänge, die Verwendung von Groß- und Kleinbuchstaben und Sonderzeichen, etc.).<sup>77</sup> Diese Vorgaben werden aber häufig auf technischer Ebene durchgesetzt, indem das System die Erstellung eines Passworts, das gegen diese Vorgaben verstößt, nicht zulässt.<sup>78</sup> I.d.R. handelt es sich daher meist um ein ganzes Maßnahmengeflecht, welches die Grenzen zwischen den Einzelmaßnahmen – und damit auch zwischen technischen und organisatorischen Maßnahmen – verschwimmen lässt.<sup>79</sup>

---

<sup>76</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 5; vgl. Schmidt/Roschek, NJW 2021, S. 367, Rn. 16 mit dem Verweis, dass organisatorische Maßnahmen die Einhaltung technischer Maßnahmen gewährleisten sollen; ähnlich aber eher mit genau entgegengesetzter Argumentation Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 72, wonach den technischen Maßnahmen gerade eine, den Prozessen unterstützende Funktion zukommt. Siehe ebenfalls BeckOK Datenschutzrecht/Schmidt/Brink, Stand: 46. Ed. 2023, Art. 24 DS-GVO (Stand: November 2023), Rn. 15, im Zusammenhang mit Art. 24 DS-GVO; auch Kipker/Reusch/Ritter/Kipker, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 24 DS-GVO, Rn. 16; Moos/Schefzig/Arning/Schefzig, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 10, Rn. 6, allgemein im Zusammenhang eines Datenschutzmanagements und daher wohl eher zu Art. 24 DS-GVO.

<sup>77</sup> Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 67; Kramer/Wenzel, IT-Arbeitsrecht, 3. Aufl. 2023, § 2, Rn. 175 f.; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 26, unter dem Punkt „Vertraulichkeit“; Forgó/Helfrich/Schneider/Schmieder, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 54; vgl. Hauschka/Moosmayer/Lösler/Schmidl, Corporate Compliance, 3. Aufl. 2016, § 28, Rn. 235, mit dem Hinweis, dass solche Richtlinien durch entsprechende Tools ersetzt werden.

<sup>78</sup> Auernhammer/Kramer/Meints, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 70; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 50; Forgó/Helfrich/Schneider/Schmieder, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 54; siehe auch Hauschka/Moosmayer/Lösler/Schmidl, Corporate Compliance, 3. Aufl. 2016, § 28, Rn. 235, wonach durch eine technische Umsetzung auf entsprechende organisatorische Vorgaben verzichtet werden kann.

<sup>79</sup> Vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 5, „abgestimmter Katalog technischer und organisatorischer Maßnahmen“; Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 5, „Paket von Maßnahmen“; Gärtner/Selzer, DuD 2023, S. 289, 290, „Maßnahmenbündel, bei dem häufig mehrere Maßnahmen zusammenwirken“.

Vor diesem Hintergrund erscheint die Klärung der Frage, ob es zwingend technischer *und* organisatorischer Maßnahmen bedarf, zunächst von nachrangiger Bedeutung, da in der Regel wohl beide Arten verwendet werden („müssen“). Eine Antwort hierauf gibt aber gleichzeitig einen tieferen Einblick in das allgemeine System des Art. 32 Abs. 1 DS-GVO, welches an späterer Stelle noch von Bedeutung sein kann.<sup>80</sup>

Der Wortlaut legt mit seiner „*und*“<sup>81</sup> Verknüpfung eine kumulative Voraussetzung nahe, wonach beide Arten von Maßnahmen implementiert werden müssten. Wie bereits angesprochen, könnte der Gesetzgeber aber auch nur ausdrücken wollen, dass beide Arten grundsätzlich zur Verfügung stünden. Aus dem Wortlaut selbst geht nicht klar hervor, dass die Datenschutz-Grundverordnung hier zwingend sowohl technische als auch organisatorische Maßnahmen zum Schutz verlangt.

Entscheidend für die Auslegung dürfte hier vor allem der Sinn und Zweck der Maßnahmen sein. Die Maßnahmen sollen das zuvor ermittelte, angemessene Schutzniveau umsetzen. Ausgehend von diesem Gedanken dürfte es jedenfalls zweifelhaft sein, warum der Gesetzgeber zwingend technische wie auch organisatorische Maßnahmen verlangen sollte. Kann das angemessene Schutzniveau bspw. nicht ausschließlich mit technischen Maßnahmen erreicht werden, so werden die Anforderungen an das angemessene Schutzniveau so lange nicht erfüllt, bis diese Lücke durch (dann) organisatorische Maßnahmen geschlossen wird. Wird andererseits jedoch das Ziel eines angemessenen Schutzniveaus mit nur einer Art von Maßnahmen erreicht, so sollte es für den Gesetzgeber keine Relevanz haben, ob hierfür nun sowohl technische als auch organisatorische Maßnahmen eingesetzt wurden oder nur eine Maßnahmenart implementiert wurde. Wichtig ist doch nur, dass das Ziel erreicht wurde.

Aufgrund dieser teleologischen Betrachtung dürfte das „*und*“ nicht dahingehend auszulegen sein, dass es – aus rein rechtlicher Sicht – zwingend erforderlich ist, sowohl technische als auch organisatorische Maßnahmen zu implementieren, um das angemessene Schutzniveau zu gewährleisten. Die Verordnung

---

<sup>80</sup> Siehe Kap. 6, A. *Der Regelungsinhalt von Art. 32 DS-GVO unter Beachtung des Problems datenverarbeitender TOM.*

<sup>81</sup> Englisch: „*and*“, Französisch: „*et*“, Spanisch: „*y*“, Italienisch: „*e*“, Niederländisch: „*en*“.

stellt mit dem „und“ lediglich klar, dass (in der Theorie) durch beide Maßnahmenarten der Schutz gewährleistet werden kann.<sup>82</sup>

Aufgrund des weiten Verständnisses der technischen und organisatorischen Maßnahmen, sowie der grundsätzlichen, rechtlichen Freiheit technische und/oder organisatorische Maßnahmen zur Gewährleistung des angemessenen Schutzniveaus zu implementieren, kann hierin jedenfalls keine Beschränkung der Maßnahmen und damit keine harte Vorgabe an diese gesehen werden.

### III. Geeignetheit der Maßnahmen

Weiterhin könnten sich Vorgaben daraus ergeben, dass es sich um *geeignete* Maßnahmen handeln muss. Auch hiermit suggeriert der Gesetzgeber, dass nicht jede Maßnahme die Pflichten des Art. 32 Abs. 1 DS-GVO erfüllen kann. Es könnte sich damit um ein qualitatives Merkmal handeln.

#### 1. Divergierende Begriffe

Beginnend mit dem Wortverständnis<sup>83</sup> dürfte man unter „geeignet“<sup>84</sup> die Fähigkeit (der Maßnahmen) verstehen, einen bestimmten Zweck (die Gewährleistung eines angemessenen Schutzniveaus) zu erfüllen. Bei der Auslegung des Begriffs i.S.d. Art. 32 DS-GVO sollte eine Fixierung auf den Wortlaut allerdings vermie-

---

<sup>82</sup> A.A. Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 9, wohl mit einer systematischen Begründung anhand der beispielhaften Aufzählungen von Maßnahmen in Art. 32 Abs. 1 Hs. 2 DS-GVO.

<sup>83</sup> Zum Wortlaut als Ausgangspunkt der Auslegung: *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 145; *Henninger*, Europäisches Privatrecht und Methode, 2009, S. 280; *Riesenhuber/Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 13; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 85; *Langenbacher/Langenbacher/Donath*, Europäisches Privat- und Wirtschaftsrecht, 5. Aufl. 2022, § 1, Rn. 10; *Roith*, RabelsZ 75 (2011), S. 787, 799; *Colneric*, ZEuP 2005, S. 225, 226; *Höpfner/Rütbers*, AcP 209 (2009), S. 1, 9; *Lutter*, JZ 1992, S. 593, 599; *Weiler*, ZEuP 2010, S. 861, 862.

<sup>84</sup> Englisch: „appropriate“, Französisch: „appropriées“, Spanisch: „apropiadas“, Italienisch: „adeguata“, Niederländisch: „passende“.

den werden. Denn auch hier zeigen sich Divergenzen im Vergleich verschiedener Sprachfassungen der Verordnung.<sup>85</sup> Besonders auffällig ist hierbei die englische Sprachfassung. Diese verwendet in Art. 32 Abs. 1 DS-GVO gleich drei Mal den Begriff „*appropriate*“, wo hingegen die deutsche Sprachfassung drei verschiedene Begriffe („*geeignet*“, „*angemessenes*“ und „*gegebenenfalls*“) verwendet. Auch die anderen untersuchten Sprachen verwenden z.T. verschiedene Begriffe für „*geeignet*“<sup>86</sup>, „*angemessenes*“<sup>87</sup> und „*gegebenenfalls*“<sup>88</sup>. Im Zusammenhang mit dem Begriff „*geeignet*“ zeigen sich aber doch auch hier sprachliche Unterschiede. Denn ähnlich wie der englische Verordnungstext dürfte sich gerade die italienische Sprachfassung eher mit dem Begriff „*angemessen*“ übersetzen lassen (Italienisch: „*adeguata*“, siehe aber auch Französisch: „*appropriées*“, Spanisch: „*apropiadas*“).<sup>89</sup>

Ausgehend vom allgemeinen Wortverständnis besteht zwischen den Begriffen „*geeignet*“ und „*angemessen*“ allerdings nach deutschem Rechtsverständnis ein erheblicher inhaltlicher Unterschied. Es handelt sich insofern nicht um Synonyme. An die „*Angemessenheit*“ dürften nach dem allgemeinen Wortverständnis höhere Anforderungen zu stellen sein als an die (bloße) „*Geeignetheit*“, da hiermit eine Abwägung und nicht nur die grundsätzliche Tauglichkeit ein Ziel zu erreichen, verbunden ist.

## 2. Maßnahmen als Mittel zum Zweck

Welches Verständnis die Datenschutz-Grundverordnung in Art. 32 Abs. 1 DS-GVO zugrunde legt und wie der Begriff „*geeignet*“ letztlich auszulegen ist, dürfte sich eher aus anderen Auslegungsarten ermitteln lassen. Aufschluss über

---

<sup>85</sup> Hierzu Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 6, der in Fn. 15 auf Basis eines Sprachvergleichs auf einen (vermeintlichen) Übersetzungsfehler in der deutschen Sprachfassung hinweist.

<sup>86</sup> Englisch: „*appropriate*“, Französisch: „*appropriées*“, Spanisch: „*apropiadas*“, Italienisch: „*adeguata*“, Niederländisch: „*passende*“.

<sup>87</sup> Französisch: „*adapté*“, Spanisch: „*adecuado*“, Italienisch: „*adeguato*“, Niederländisch: „*afgestemd*“.

<sup>88</sup> Französisch: „*selon les besoins*“, Spanisch: „*en su caso*“, Italienisch: „*se del caso*“, Niederländisch: „*waar passend*“.

<sup>89</sup> Siehe hierzu auch die Einschätzung von Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 6, in Fn. 15 zum Vergleich der englischen, französischen, niederländischen und italienischen Sprachfassung.

das Verständnis könnten hier vor allem die teleologische Auslegung und die Systematik des Art. 32 Abs. 1 DS-GVO geben. Aus der Systematik von Art. 32 Abs. 1 DS-GVO ergibt sich, dass die Maßnahmen die Umsetzung des angemessenen Schutzniveaus gewährleisten sollen. Der daraus abzuleitende Zweck der Maßnahmen besteht folglich darin, dass sie das tatsächliche Mittel sind, das rechtliche Ziel zu erreichen.

Damit die Maßnahmen ihren Zweck erfüllen können, muss es sich folglich auch um solche Maßnahmen handeln, die einen Beitrag zur Gewährleistung des angemessenen Schutzniveaus leisten können.<sup>90</sup> Das bedeutet, dass die Maßnahmen den Eintritt eines personal data breaches und / oder dessen Auswirkungen auf die Rechte und Freiheiten betroffener Personen verhindern oder jedenfalls abmildern können sollten.

Die Funktion, die die Datenschutz-Grundverordnung den Maßnahmen im Rahmen des Art. 32 Abs. 1 DS-GVO zugedenkt, dürfte damit wohl eher dem allgemeinen Wortverständnis der „Geeignetheit“ entsprechen. Sie müssen demnach einen Beitrag zur Gewährleistung des angemessenen Schutzniveaus leisten. Einer gesonderten Abwägung, die im Rahmen einer (weiteren) Angemessenheitsprüfung erforderlich wäre, bedarf es demnach nicht. Vor allem nicht durch die (zuvor genannten) Kriterien gleich zu Beginn des Art. 32 Abs. 1 DS-GVO. Da sich diese bereits in dem angemessenen Schutzniveau manifestieren.<sup>91</sup>

Können die (einzelne) Maßnahmen keinen Beitrag zum angemessenen Schutzniveau leisten oder in ihrer Gesamtheit dieses nicht gewährleisten, so wären sie auch nicht geeignet, die Pflichten aus Art. 32 Abs. 1 DS-GVO zu erfüllen.

### 3. Die „Geeignetheit“ als Einschränkung?

Ob man nach alledem bei der „Geeignetheit“ der Maßnahmen von einer wirklichen Vorgabe an die zu treffenden Maßnahmen sprechen kann, dürfte damit

---

<sup>90</sup> Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 36; vgl. Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10, „*Umsetzung der Ziele des Art. 32*“; wohl ähnlich *Jandt*, DuD 2017, S. 562, 563, wonach sich die Geeignetheit auf „*das Ziel der Risikoreduzierung*“ bezieht; Schwartmann u.a./*Ritter*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 82; in eine ähnliche Richtung *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 3.

<sup>91</sup> Siehe zu dieser Herleitung: Kap. 5, B., III. *Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?*

jedoch zu bezweifeln sein. Tragen die Maßnahmen nichts zur Gewährleistung des angemessenen Schutzniveaus bei, so wird dieses auch nicht erfüllt. Diese Konsequenz ergibt sich aber bereits aus der Pflicht selbst. Dafür hätte es einen Tatbestand wie die „Geeignetheit“ der Maßnahmen nicht unbedingt gebraucht. Regelungstechnisch könnte die „Geeignetheit“ der Maßnahmen damit wohl eher ein Hinweis auf die enge Verbindung des angemessenen Schutzniveaus und dessen Umsetzung mittels technischer und organisatorischer Maßnahmen sein.<sup>92</sup> Dies könnte auch gerade den abweichenden Begriff der „Angemessenheit“ in einigen Sprachfassungen erklären, da schließlich das Schutzniveau dieser Angemessenheitsprüfung unterliegt und die Maßnahmen dieses angemessene Schutzniveau gewährleisten müssen. Das darf aber weder dahingehend verstanden werden, dass auf der Ebene der Maßnahmen eine (erneute) Angemessenheitsprüfung vorzunehmen ist. Noch kann man in der „Geeignetheit“ oder „Angemessenheit“ der Maßnahmen eine gesetzliche Vorgabe dahingehend verstehen, dass hierüber ausgesagt wird, welche Maßnahmen getroffen werden müssen oder eine Einschränkung auf bestimmte Maßnahmen erfolgen soll.<sup>93</sup>

#### *IV. Anforderungen an die Maßnahmen nach Art. 32 Abs. 1 Hs. 2 DS-GVO*

Eine echte Vorgabe an die technischen und organisatorischen Maßnahmen könnte sich schließlich aus Art. 32 Abs. 1 Hs. 2 DS-GVO ergeben. Art. 32 Abs. 1 Hs. 2 DS-GVO enthält eine Auflistung von vier Punkten, die es wohl bei der Implementierung von Maßnahmen zu berücksichtigen gilt. Fraglich ist aber auch hier wieder, ob die Verordnung mit dieser Aufzählung „harte“ Vorgaben an die Maßnahmen und deren Implementierung stellt.

---

<sup>92</sup> Wohl in eine ähnliche Richtung argumentieren Kipker/Reusch/Ritter/*Piltz/Zwerschke*, *Recht der Informationssicherheit*, 2023, *Datenschutz-Grundverordnung*, Art. 32 DS-GVO, Rn. 36; Gola/Heckmann/*Piltz*, *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, Art. 32 DS-GVO, Rn. 12., indem er eine Verbindung zum angemessenen Schutzniveau zieht. Siehe auch: Sydow/Marsch/*Mantz*, *DS-GVO – BDSG*, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 6 (und Fn. 15), mit dem Hinweis auf eine „*Fehlübersetzung*“ der deutschen Fassung und dem Verweis auf „*angemessene technische und organisatorische Maßnahmen*“, was damit die gedankliche Verbindung zum angemessenen Schutzniveau aufkommen lässt.

<sup>93</sup> Ehmann/Selmayr/*Hladjk*, *Datenschutz-Grundverordnung*, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 4; Kiparski/*Zirfas*, *CR* 2021, S. 108, Rn. 19; Freund u.a./*Freund/Schöning*, *DSGVO*, 2023, Art. 32 DS-GVO, Rn. 42, wonach hiermit „*lediglich völlig unwirksame Maßnahmen*“ ausgeschlossen werden sollen; ähnlich Kühling/*Buchner/Jandt*, *DS-GVO – BDSG*, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 8.

### 1. Relativierung des „Verbindlichkeitsgrads“?

Bevor auf die einzelnen Punkte eingegangen werden soll, verdient bereits der einleitende Satz einer genaueren Betrachtung. Denn schon an dieser Stelle erweckt die Verordnung den Eindruck, dass die nachfolgenden Vorgaben an die Maßnahmen wohl nicht zwingend sein sollen.

Zunächst verweist die Verordnung mit der Formulierung „*unter anderem*“<sup>94</sup> darauf, dass es sich nachfolgend um eine nicht abschließende Aufzählung handelt.<sup>95</sup> Von größerer Bedeutung ist jedoch die Verwendung des Begriffs „*gegebenenfalls*“<sup>96</sup>. Im Kontext gesehen heißt es:

„[...] *schließen gegebenenfalls unter anderem Folgendes ein: [...]*“<sup>97</sup>.

Daraus lässt sich zunächst ableiten, dass die nachfolgenden Punkte auch nicht zwingend bei der Implementierung der Maßnahmen einzuhalten sind.<sup>98</sup>

<sup>94</sup> Englisch: „*inter alia*“, Französisch: „*entre autres*“, Spanisch: „*entre otros*“, Italienisch: „*tra le altre*“, Niederländisch: „*onder meer*“.

<sup>95</sup> John/Schaller, CR 2022, S. 156, 156; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 3; wohl auch mit Verweis auf diese Formulierung Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 14; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 9, mit allgemeinem Verweis auf den Wortlaut; im Ergebnis auch: Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 6; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 31; DatKomm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 45; siehe auch Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 24 f., verweist jedoch nicht konkret bezüglich des nicht abschließenden Charakters auf diese Formulierung.

<sup>96</sup> Englisch: „*as appropriate*“, Französisch: „*selon les besoins*“, Spanisch: „*en su caso*“, Italienisch: „*se del caso*“, Niederländisch: „*waar passend*“.

<sup>97</sup> Englisch: „[...] *including inter alia as appropriate: [...]*“, Französisch: „[...] *y compris entre autres, selon les besoins: [...]*“, Spanisch: „[...] *que en su caso incluya, entre otros: [...]*“, Italienisch: „[...] *che comprendono, tra le altre, se del caso: [...]*“, Niederländisch: „[...] *waar passend, onder meer het volgende omvatten: [...]*“.

<sup>98</sup> Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 24; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 44; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 14;



Dies könnte der Einordnung als „harte“ Vorgaben an die Maßnahmen entgegenstehen.

Der Gesetzgeber dürfte dem Wort „gegebenenfalls“ bei der Auslegung des Art. 32 Abs. 1 DS-GVO eine zentrale Funktion zumessen. Dies lässt sich daraus ableiten, dass wenigstens die frühere deutsche Fassung der Datenschutz-Grundverordnung diesen Zusatz nicht enthielt.<sup>99</sup> Der Gesetzgeber hat dies als einen Übersetzungsfehler behandelt und durch eine Berichtigung der Verordnung<sup>100</sup> nachträglich korrigiert.<sup>101</sup> Dass der Gesetzgeber hier extra eine Berichtigung der Verordnung vorgenommen hat, zeigt, dass es sich bei dem Begriff nicht um ein (grundsätzlich zu vermeidendes)<sup>102</sup> Füllwort oder seinerseits um einen Übersetzungsfehler handelt. Der Begriff sollte vielmehr zwingend bei der Auslegung beachtet werden. Konsequenz ist, dass die Verordnung bereits im Einleitungssatz des Art. 32 Abs. 1 Hs. 2 DS-GVO die nachfolgend aufgeführten Vorgaben an die Maßnahmen relativiert.

## 2. Überblick über die inhaltlichen Vorgaben

Die Aufzählung nach Art. 32 Abs. 1 Hs. 2 DS-GVO umfasst insgesamt nur vier Punkte. Diese vier Punkte lassen sich in drei Kategorien unterteilen.<sup>103</sup>

---

Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 32; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 31. Siehe zu einer möglichen Differenzierung sogleich, Kap. 5, C., IV., 3. *Art. 32 Abs. 1 Hs. 2 DS-GVO als unverbindliche Orientierungshilfe*.

<sup>99</sup> Auf die Diskrepanz zwischen den Sprachfassungen wies Gola/Piltz, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 32 DS-GVO, Rn. 24 bereits vor der Änderung hin.

<sup>100</sup> Berichtigung der Datenschutz-Grundverordnung, ABl. EU L. 127, vom 23.05.2018, S. 2 ff.

<sup>101</sup> Berichtigung der Datenschutz-Grundverordnung, ABl. EU L. 127, vom 23.05.2018, S. 2, 4; BeckOK Datenschutzrecht/Paulus, Stand: 46. Ed. 2023, Art. 32 DS-GVO (Stand: November 2021), Rn. 1; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 18a; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 8.

<sup>102</sup> Europäische Union, Gemeinsamer Leitfaden für das Abfassung von Rechtstexten, 2015, DOI 10.2880/836230, Leitlinie 1.1; siehe auch Peifer, Bessere Rechtssetzung als Leitbild europäischer Gesetzgebung, 2011, S. 78 ff., zu den Anforderungen, aus dem Grundsatz der Rechtssicherheit folgenden „Bestimmtheitsgebot“ beim Verfassen von Rechtsnormen.

<sup>103</sup> Vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 16 spricht hier von einem „unterschiedlich hohen technischen Konkretisierungsgrad“; ähnlich Gärtner/Selzer, DuD 2023, S. 289, 290; vgl. auch Paal/Pauly/Martini, DS-GVO BDSG, 3.

a) Pseudonymisierung und Verschlüsselung (lit. a))

Mit der „Pseudonymisierung“<sup>104</sup> und der „Verschlüsselung“<sup>105</sup> listet lit. a) zwei Maßnahmen auf, die Sicherheit der Verarbeitung zu gewährleisten.<sup>106</sup>

Der Begriff der Verschlüsselung wird von der Verordnung nicht definiert.<sup>107</sup> Bei der Verschlüsselung von Daten werden mithilfe eines mathematischen Verfahrens die Daten so abgeändert, dass ihr ursprünglicher Inhalt nicht mehr ausgelesen werden kann, außer mit Hilfe des entsprechenden Schlüssels.<sup>108</sup> Aus der Perspektive der Sicherheit der Verarbeitung kann eine Verschlüsselung den unberechtigten Zugriff auf die Daten (bzw. eher ihren eigentlichen Inhalt) verhindern.<sup>109</sup>

---

Aufl. 2021, Art. 32 DS-GVO, Rn. 30, der von „konkrete“ und „abstrakte“ Maßnahmen spricht, dabei aber (als mögliche 3. Gruppe) lit. d) nicht gesondert erwähnt.

<sup>104</sup> Englisch: „pseudonymisation“, Französisch: „pseudonymisation“, Spanisch: „seudonimización“, Italienisch: „pseudonimizzazione“, Niederländisch: „pseudonimiseren“.

<sup>105</sup> Englisch: „encryption“, Französisch: „chiffrement“, Spanisch: „cifrado“, Italienisch: „cifatura“, Niederländisch: „versleuteling“.

<sup>106</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 16; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 30; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 12; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 6; Gärtner/Selzer, DuD 2023, S. 289, 290, jedenfalls ausdrücklich auf die Pseudonymisierung verweisend; vgl. auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 31, die in Fn. 32 jedenfalls darauf verweist, dass es sich bei lit. b) und lit. c) nicht um Maßnahmen handle.

<sup>107</sup> Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 35, allerdings mit Verweis auf Art. 34 Abs. 3 lit. a) DS-GVO, wonach das Konzept der Verschlüsselung dort grob erklärt wird; so auch Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 48.

<sup>108</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 19; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 34; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11; Hornung/Schallbruch/Grimm/Waidner, IT-Sicherheitsrecht, 2021, § 2, Rn. 91 ff.; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 5; Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 19a. Ausführlicher zur Verschlüsselung: Küppers, Einführung in die Informatik, 2022, S. 165 ff.

<sup>109</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 34; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 35; v.d.

Für die Verschlüsselung von Daten stehen verschiedene Verfahren, wie die symmetrische und asymmetrische Verschlüsselung zur Verfügung.<sup>110</sup> Welches Verschlüsselungsverfahren einzusetzen ist, bzw. allgemein wie die Verschlüsselung überhaupt zu erfolgen hat, wird in der Datenschutz-Grundverordnung nicht vorgegeben.<sup>111</sup>

Das Konzept der Pseudonymisierung wird in Art. 4 Nr. 5 DS-GVO definiert. Dabei handelt es sich um ein Verfahren, bei der die personenbezogenen Elemente von den übrigen Daten eines Datensatzes getrennt werden, sodass die Daten der betroffenen Person nur noch unter Zuhilfenahme dieser zusätzlichen Informationen zugeordnet werden können.<sup>112</sup> Dies kann bspw. damit erreicht werden, indem (sehr vereinfacht beschrieben) ein Name in einem Datensatz durch eine Kennnummer ausgetauscht wird, aber in einem davon getrennten Datensatz der Name dann der Kennnummer zugeordnet ist.<sup>113</sup> Anders als bei

---

Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 5; Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 178.

<sup>110</sup> Buchmann, Einführung in die Kryptographie, 6. Aufl. 2016, S. 73 ff., 165 ff., wobei die asymmetrische Verschlüsselung dort überwiegend als „Public-Key Verschlüsselung“ bezeichnet wird; Paar/Pelzl, Kryptografie verständlich, 2016, S. 3 ff., 173 ff.; Küsters/Wilke, Moderne Kryptographie, 2011, S. 7 f., 13 ff., 137 ff.; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 34a; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 19; Kipker/Sohr/Kemmerich, Cybersecurity, 2. Aufl. 2023, Kapitel 3, Rn. 33 ff.; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 48; Gierschmann u.a./Jergl, Datenschutz-Grundverordnung, 2018, Art. 32 DS-GVO, Rn. 23 ff.

<sup>111</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 20 f.; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 27; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 12, als Ausdruck des „Grundsatz der Technikneutralität“; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 49.

<sup>112</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 33; Gierschmann u.a./Jergl, Datenschutz-Grundverordnung, 2018, Art. 32 DS-GVO, Rn. 22; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 4; Hansen/Walczak, RDV 2019, S. 53, 53 f.; Roßnagel, ZD 2018, S. 243, 243; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 18.

<sup>113</sup> Vgl. Hansen/Walczak, RDV 2019, S. 53, 53 f.; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 18.

einer Anonymisierung ist eine Zuordnung der Daten zu einer bestimmten Person weiterhin möglich.<sup>114</sup>

Mit Blick auf die Sicherheit der Verarbeitung kann auch die Pseudonymisierung dazu beitragen, die Risiken bspw. eines unbefugten Zugriffs zu minimieren, indem es der unbefugten Person erschwert wird, die Erkenntnisse aus den Daten einer bestimmten Person zuzuordnen.<sup>115</sup> Wichtig dabei ist allerdings, dass i.S.d. Definition nach Art. 4 Nr. 5 DS-GVO die Informationen, die einen Personenbezug wiederherstellen können, getrennt und sicher von dem (pseudonymisierten) Datensatz aufbewahrt werden.<sup>116</sup>

Auch für die Pseudonymisierung können verschiedene Verfahren angewendet werden.<sup>117</sup> Abgesehen von der allgemeinen Beschreibung in Art. 4 Nr. 5 DS-

---

<sup>114</sup> Ehmann/Selmayr/*Klabunde*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 33; v.d. Bussche/Voigt/*Voigt*, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 4; Taeger/Gabel/*Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 55; Hansen/*Walczak*, RDV 2019, S. 53, 53 f.; Sydow/Marsch/*Ziebarth*, DS-GVO – BDSG, 3. Aufl. 2022 Art. 4 DS-GVO, Rn. 93; vgl. *Schleipfer*, ZD 2020, S. 284, 285. Siehe jedoch zu unterschiedlichen – auch anonymisierenden – Wirkungen einer Pseudonymisierung *Rofsnagel*, ZD 2018, S. 243, 245 f.; siehe auch Hansen/*Walczak*, RDV 2019, S. 53, 55.

<sup>115</sup> Auernhammer/*Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 25; Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 11; vgl. Simitis/Hornung/Spiecker gen. Döhmman/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 34; Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 32.

<sup>116</sup> Simitis/Hornung/Spiecker gen. Döhmman/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 34; Kühling/Buchner/*Klar/Kübling*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 5 DS-GVO, Rn. 6 f.; DatKomm/*Hödl*, Stand: 76. EL. 2023, Art. 4 DS-GVO (Stand: Februar 2019), Rn. 60; Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 32.

<sup>117</sup> Kühling/Buchner/*Klar/Kübling*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 5 DS-GVO, Rn. 8; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 18; Hansen/*Walczak*, RDV 2019, S. 53, 56 f.; Simitis/Hornung/Spiecker gen. Döhmman/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 34. Siehe auch zu unterschiedlichen Arten bzw. Ansätzen einer Pseudonymisierung: *Rofsnagel/Scholz*, MMR 2000, S. 721, 725; *Schleipfer*, ZD 2020, S. 284 ff.; BeckOK Datenschutzrecht/*Schild*, Stand: 46. Ed. 2023, Art. 4 DS-GVO (Stand: November 2023), Rn. 74 ff.; Taeger/Gabel/*Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 144 ff.

GVO wonach jedenfalls die zwei Kernvoraussetzungen (Trennung des Personenbezugs und gesonderte, sichere Aufbewahrung)<sup>118</sup> erfüllt sein müssen, macht die Verordnung auch hier keine konkreten Vorgaben hinsichtlich bestimmter Pseudonymisierungsverfahren.<sup>119</sup> Insofern handelt es sich bei dem Verweis auf die Pseudonymisierung und Verschlüsselung in Art. 32 Abs. 1 Hs. 2 lit. a) DS-GVO wohl eher um Maßnahmenkategorien als konkrete Maßnahmen, die die Verordnung hier aufzählt.

---

<sup>118</sup> Vgl. *Roßnagel*, ZD 2018, S. 243, 246; siehe auch *DatKomm/Hödl*, Stand: 76. EL. 2023, Art. 4 DS-GVO (Stand: Februar 2019), Rn. 58, die diese Anforderung in drei Teile (getrennt und sicher) aufteilt; ebenso *Paal/Pauly/Ernst*, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 DS-GVO, Rn. 41 ff.; auch *Specht/Mantz/Schneider*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 15, Rn. 86 ff.; siehe auch *Hansen/Walczak*, RDV 2019, S. 53, 54 f., die die zwei Kernanforderungen allerdings dahingehend ergänzen, dass die Pseudonymisierung dem Stand der Technik entsprechen müsse.

<sup>119</sup> *Roßnagel*, ZD 2018, S. 243, 246; *Kipker/Reusch/Ritter/Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 45; *Hansen/Walczak*, RDV 2019, S. 53, 54; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 12, als Ausdruck des „Grundsatz der Technikneutralität“; vgl. *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 33a, der darauf verweist, dass sich die „geeignete Pseudonymisierungsmethode“ gerade nach den Umständen richte.

*b) Fähigkeit zur Gewährleistung der Ziele: Vertraulichkeit, Integrität, Verfügbarkeit (und Belastbarkeit) (lit. b) und c))*

In lit. b) und c) beschreibt die Verordnung keine konkreten Maßnahmen oder Maßnahmenkategorien, sondern konkretisiert vielmehr, über welche „Fähigkeiten“ die Maßnahmen verfügen sollen.<sup>120</sup> Hierzu gehören nach lit. b) die „Vertraulichkeit“<sup>121</sup>, „Integrität“<sup>122</sup>, „Verfügbarkeit“<sup>123</sup> und „Belastbarkeit“<sup>124</sup> der datenverarbeitenden Systeme und Dienste sowie nach lit. c) die Wiederherstellung der „Verfügbarkeit“<sup>125</sup> der Daten selbst, nach einem Zwischenfall. Gerade die Oberbegriffe „Verfügbarkeit“, „Integrität“ und „Vertraulichkeit“ stehen in einem engen Zusammenhang mit den Gefahren eines personal data breach (und damit des Ziels von Art. 32 DS-GVO)<sup>126</sup>, wie es insbesondere in Art. 32 Abs. 2 DS-GVO zum Ausdruck gebracht wird.<sup>127</sup> Insofern ist es auch fast selbstverständlich, dass die Maßnahmen zur Erfüllung dieses Ziels über diese Fähigkeiten

<sup>120</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 16; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 31, Fn. 32; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 30 spricht hier von „abstrakten Maßnahmen“ bzw. „Zielvorgaben“; ebenfalls von „Zielvorgaben“ spricht v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 6, 12; Roßnagel/Husemann, Das neue Datenschutzrecht, 2018, § 5, Rn. 138, kritisiert gerade das gleichwertige Nebeneinander von „Maßnahmen“ und „Datensicherheitszielen“; Gärtner/Selzer, DuD 2023, S. 289, 290, sprechen ebenfalls von abstrakten „Datensicherheitszielen“, ohne diese jedoch konkret dem Katalog zuzuordnen.

<sup>121</sup> Englisch: „confidentiality“, Französisch: „la confidentialité“, Spanisch: „la confidencialidad“, Italienisch: „la riservatezza“, Niederländisch: „de vertrouwelijkheid“.

<sup>122</sup> Englisch: „integrity“, Französisch: „l'intégrité“, Spanisch: „integridad“, Italienisch: „l'integrità“, Niederländisch: „integriteit“.

<sup>123</sup> Englisch: „availability“, Französisch: „la disponibilité“, Spanisch: „disponibilidad“, Italienisch: „la disponibilità“, Niederländisch: „beschikbaarheid“.

<sup>124</sup> Englisch: „resilience“, Französisch: „la résilience“, Spanisch: „resiliencia“, Italienisch: „la resilienza“, Niederländisch: „veerkracht“.

<sup>125</sup> Englisch: „availability“, Französisch: „la disponibilité“, Spanisch: „la disponibilidad“, Italienisch: „la disponibilità“, Niederländisch: „beschikbaarheid“.

<sup>126</sup> Siehe hierzu bereits: Kap. 4, C., II. Die Bedeutung des Begriffs „personal data breach“ und III. Anwendung auf (andere) Sicherheitsvorfälle.

<sup>127</sup> Siehe bereits die Verbindung dieser „Schutzziele“ mit der groben Einordnung des Art. 32 DS-GVO als Gewährleistung der „Datensicherheit“ unter Kap. 4, A. Sicherheit der Verarbeitung, Datensicherheit, Informationssicherheit, etc.; siehe auch Simitis/Hornung/Spiecker gen.

verfügen müssen. Andernfalls wären sie auch nicht dafür geeignet. Art. 32 Abs. 1 Hs. 2 lit. b) und lit. c) DS-GVO heben daher noch einmal das Regelungsziel hervor.<sup>128</sup> Eine solche „Konkretisierung“ wäre allerdings nicht nötig gewesen, käme das Regelungsziel bereits aus dem restlichen Verordnungstext eindeutiger hervor.<sup>129</sup>

c) Überprüfungsverfahren (lit. d))

Abschließend wird in lit. d) noch aufgeführt, dass die entsprechenden Maßnahmen nicht nur einmal getroffen werden sollen, sondern gleichzeitig auch ein Überprüfungssystem einzuführen ist, um die Wirksamkeit der Maßnahmen laufend zu überwachen und ggf. Anpassungen vorzunehmen. Auch hier ist fraglich, ob eine solche „Konkretisierung“ erforderlich wäre. An die Wirksamkeit der Maßnahmen knüpft direkt auch die Erfüllung des angemessenen Schutzniveaus nach Art. 32 Abs. 1 DS-GVO insgesamt an. Verlieren einmal getroffene Maßnahmen im Zeitablauf ihre Wirksamkeit und wird hierdurch das angemessene Schutzniveau nicht länger gewährleistet, so besteht die Pflicht, Anpassungen vorzunehmen.<sup>130</sup> Die Sicherheit der Verarbeitung ist damit grundlegend

---

Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 31, dass lit. b) – lit. d) zu den „Standardanforderungen“ des angemessenen Schutzniveaus gehören.

<sup>128</sup> Siehe allgemein, dass sich aus den Beispielen des Art. 32 Abs. 1 Hs. 2 lit. a) - d) DS-GVO auf die zu adressierten „Risiken“ schließen lässt Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 58.

<sup>129</sup> Siehe zu dieser Kritik bereits oben: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO*.

<sup>130</sup> Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 18; vgl. v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 26; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 73. Vielfach wird dies gerade aus dem Tatbestand „Stand der Technik“ abgeleitet, der insofern eine entsprechende Dynamik aufweise: Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 9; Ehmann/Selmayr/Hladjke, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 5 f.; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 21; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 6; Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 19d; Taeger/Gabel/Schultze-Melling, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 13; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 73; Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 151 f.; Knopp, DuD 2017, S. 663, 666.

eine dauerhafte Verpflichtung, solange die zu schützenden, personenbezogenen Daten verarbeitet werden.<sup>131</sup> Daraus ergibt sich faktisch auch die „Pflicht“, Überwachungs- und Kontrollsysteme zu etablieren, um den Anforderungen an die Sicherheit der Verarbeitung auch laufend gerecht zu werden.<sup>132</sup>

### 3. Art. 32 Abs. 1 Hs. 2 DS-GVO als unverbindliche Orientierungshilfe

Sowohl der einleitende Text zu Art. 32 Abs. 1 Hs. 2 DS-GVO als auch der Inhalt der Aufzählung lassen daran zweifeln, dass der Gesetzgeber hier besondere Vorgaben an die Maßnahmen stellen wollte. Auch wenn der Einleitungssatz von Art. 32 Abs. 1 Hs. 2 DS-GVO deutlich macht, dass die aufgeführten Punkte nicht zwingend sind, wird ihnen in Teilen der Literatur dennoch eine besondere Stellung zugedacht. So wird vertreten, dass dadurch, dass der Gesetzgeber sie gesondert auflistet, sie auch im Auswahlprozess zwingend zu berücksichtigen seien.<sup>133</sup> Ob Art. 32 Abs. 1 Hs. 2 DS-GVO jedoch eine so große Bedeutung zukommt, lässt sich bezweifeln. Hiergegen spricht einmal die Relativierung in der

<sup>131</sup> Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 18; v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 26; vgl. Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 12; vgl. auch Jahnelt/Bergauer, DSGVO, 2021, Art. 32 DS-GVO, Rn. 2, „zu jeder Zeit der Verarbeitung“; siehe auch Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 43 und spricht hier von einer „*normativen Leitidee*“; so auch Heidrich, Stresstest für die DSGVO, in: Den Wandel begleiten, 2020, S. 391, 398.

<sup>132</sup> Vgl. auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, Art. 32 DS-GVO, Rn. 18; siehe auch Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 73, wonach die Pflicht zur Überprüfung „*nicht erst aufgrund des lit. d*“ besteht; siehe zudem Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 43, wonach diese Verpflichtung sich aus „*der normativen Leitidee*“ ergibt; so auch Heidrich, Stresstest für die DSGVO, in: Den Wandel begleiten, 2020, S. 391, 398; v. Lewinski/Rüpke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 26, sehen daher in Art. 32 Abs. 1 lit. d) DS-GVO eher eine Klarstellung; siehe zudem Wybitul/Schreibauer/Spitka, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 32 DS-GVO, Rn. 14, die ebenfalls von einer Klarstellung sprechen.

<sup>133</sup> Kuner/Bygrave/Docksey/Burton, GDPR, 2020, p. 636, sieht hier den Ausdruck einer Präferenz und entsprechenden Erwartungen diese soweit es geht zu implementieren; ähnlich Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 32, der zudem von „*Mindestvorgaben*“ spricht, aber auch klarstellt, dass diese im Einzelfall nicht zwingend sind; auch mit Verweis auf einen „*Mindeststandard*“ Albrecht/Jotzo, Das neue Datenschutzrecht der



Verordnung selbst. Weiterhin sind aber auch drei (lit. b), c), d)) Punkte schlicht obsolet. Denn deren maßgeblicher Inhalt lässt sich bereits aus dem allgemeinen Zweck des Art. 32 Abs. 1 DS-GVO ableiten und bedarf daher eigentlich keiner zusätzlichen Berücksichtigung bei den Maßnahmen. Aufgrund der Ableitung aus dem allgemeinen Schutzzweck müssen die Maßnahmen zwar diese Aspekte beachten, um ein angemessenes Schutzniveau gewährleisten zu können. Es handelt sich aber nicht um „zusätzliche“ Anforderungen an die Maßnahmen selbst.

In Bezug auf die einzigen beiden, „konkreten“ Maßnahmen(-kategorien), der Pseudonymisierung und Verschlüsselung, dürfte es, in Anbetracht der Vielzahl denkbarer Maßnahmen und der unterschiedlichen Risiken, schon fast problematisch sein, wenn die Verordnung sich hier nur auf zwei „Vorschläge“ oder „Vorgaben“ konzentriert.<sup>134</sup> Zumal es sich auch scheinbar um die einzigen Maßnahmen(-kategorien) handelt, die der Gesetzgeber überhaupt ausdrücklich anspricht, da auch an anderer Stelle allenfalls nur die Rede von der Pseudonymisierung und der Verschlüsselung ist.<sup>135</sup> Hieraus priorisierte Maßnahmen(-kategorien) abzuleiten, die als „Allzweckwerkzeug“ dienen sollen, dürfte zu weit gehen.<sup>136</sup>

Aufgrund des bereits sehr relativierenden Einleitungssatzes, zusammen mit den teils eher klarstellenden Beispielen, ist Art. 32 Abs. 1 Hs. 2 DS-GVO nicht dahingehend auszulegen, dass der Gesetzgeber mit seiner Auflistung vorhatte, bestimmte Vorgaben an die technischen und organisatorischen Maßnahmen zu machen, die sich nicht bereits aus dem allgemeinen Inhalt des Art. 32 Abs. 1 DS-

---

EU, 2017, Teil 5, Rn. 9; siehe in diese Richtung auch v.d. Bussche/Voigt/Voigt, *Konzerndatenschutz*, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 2 ff.; jedenfalls für die Implementierung von Pseudonymisierung und Verschlüsselung wohl auch Sydow/Marsch/Mantz, *DS-GVO – BDSG*, Art. 32 DS-GVO, Rn. 11. Siehe auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, *Datenschutzrecht*, Art. 32 DS-GVO, Rn. 31, wobei die Begründung vorrangig daran anknüpft, dass es sich hier um Standardanforderungen handle.

<sup>134</sup> Roßnagel/Husemann, *Das neue Datenschutzrecht*, 2018, § 5, Rn. 138; ebenfalls kritisch Gierschmann u.a./Jergl, *Datenschutz-Grundverordnung*, 2018, Art. 32 DS-GVO, Rn. 29.

<sup>135</sup> Die Verschlüsselung und die Pseudonymisierung werden neben Art. 32 DS-GVO noch gemeinsam in Art. 6 Abs. 4 lit. e) DS-GVO erwähnt. Dazu wird auf die Verschlüsselung noch in Art. 34 Abs. 3 lit. a) DS-GVO und die Pseudonymisierung noch in Art. 25 Abs. 1, 40 Abs. 2 lit. d) und 89 Abs. 1 DS-GVO Bezug genommen.

<sup>136</sup> Siehe auch *Schleipfer*, ZD 2020, S. 284, 289, ebenfalls kritisch zur Pseudonymisierung als „Allzweck-Wunderwaffe“, aber im Kontext der gesamten Verordnung.

GVO ergeben hätten. Der Auflistung dürfte damit allenfalls eine Orientierungsfunktion zukommen.<sup>137</sup>

### *V. Telos als Basis gesetzgeberischer Vorgaben*

Nach der hier vertretenen Ansicht stellt die Datenschutz-Grundverordnung in Art. 32 DS-GVO keine nennenswerten Vorgaben an die Implementierung technischer und organisatorischer Maßnahmen. Die Ausführungen, die die Verordnung in diesem Zusammenhang macht, können allenfalls als Art Orientierungshilfe dienen, Maßnahmen zu treffen, die in der Lage sind, das angemessene Schutzniveau sicherzustellen. Zusätzliche Anforderungen, die über diese Funktion hinausgehen, werden Datenverarbeitern hingegen nicht auferlegt.

Abgesehen von den Regelungen, die der Gesetzgeber in diesem Zusammenhang erlassen hat, verdient abschließend eine kurze, allgemein teleologische Überlegung Beachtung, warum gesetzgeberische Vorgaben an die Implementierung technischer und organisatorischer Maßnahmen auch schlicht keinen Sinn ergeben würden. Sie könnten dem Regelungsziel sogar zuwiderlaufen. Dabei sollten drei Punkte beachtet werden.

#### *1. Gefahr des Widerspruchs zwischen Vorgaben und Ziel*

Ein wichtiger Punkt, den es zu berücksichtigen gilt, ist der Einfluss des (vor allem technologischen) Wandels auf die Sicherheit der Verarbeitung. Die Wirksamkeit einer Vielzahl von Maßnahmen wandelt sich im Laufe der Zeit.<sup>138</sup> Zur Veranschaulichung dient hier besonders gut die – sogar in Art. 32 Abs. 1, Hs. 2 lit a) DS-GVO benannte – Verschlüsselung. Die Wirksamkeit von Verschlüsselungen hängt u.a. von der speziellen Verschlüsselungsart und der Schlüssellänge

---

<sup>137</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 14; Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 25; vgl. auch Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 44, die eine Berücksichtigung der Beispiele aber im „*eigenen Interesse*“ der Verpflichteten sehen.

<sup>138</sup> Siehe hierzu bereits oben die Ausführungen zur dauerhaften Gewährleistung des Schutzniveaus und dort vor allem die zitierte Ansicht, dass sich dieser Wandel gerade im Rahmen des Tatbestands „*Stand der Technik*“ manifestiere: Statt vieler Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 9 und die weiteren Nachweise in Kap. 5, C., IV., 2., c) *Überprüfungsverfahren (lit. d)*) und dort insb. Fn. 130. Siehe auch *Marschall*, DuD 2015, S. 183, 189, der bspw. im Fall kryptografischer Maßnahmen von „*Verfallsdatum*“ spricht.

ab.<sup>139</sup> Gerade in Bezug auf die Schlüssellänge hat der Fortschritt in der Informationstechnik dazu geführt, dass für eine sichere Verschlüsselung mittlerweile längere Schlüssel (bspw. 256 Bit anstelle von 128 Bit)<sup>140</sup> erforderlich sind als noch in der Vergangenheit.<sup>141</sup> Aufgrund der heute leistungsstärkeren Systeme der Informationstechnik wäre es viel leichter und schneller möglich, durch ausprobieren aller möglichen Kombinationen (sog. „Brute Force Attacken“<sup>142</sup>) eine Verschlüsselung mit kurzer Schlüssellänge zu entschlüsseln.<sup>143</sup> Der Schutz den solche Verschlüsselungsverfahren in der Vergangenheit hatten, liegt unter den heutigen Umständen nicht länger vor. Weiterhin könnten auch neue Technologien entwickelt werden, die den bestehenden Schutz aushebeln könnten.

Würde der Gesetzgeber in diesem dynamischen Bereich (konkrete) rechtliche Vorgaben an die zu treffenden Maßnahmen machen, liefe er Gefahr, sein eigenes, gesetztes Ziel eines angemessenen Schutzniveaus selbst zu schaden bzw. einen Konflikt innerhalb der Norm zu erzeugen.<sup>144</sup>

---

<sup>139</sup> Vgl. Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 17; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 34a, 34c f.; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 19, 21; Forgó/Helfrich/Schneider/*Schmieder*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 2, Rn. 70 anhand von Übermittlungsverschlüsselungen; siehe zur Bedeutung der Schlüssellänge auch Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 49.

<sup>140</sup> Siehe zu den Empfehlungen des BSI zur Schlüssellänge für verschiedene Verschlüsselungsverfahren: BSI, TR-02102-1.

<sup>141</sup> Siehe hierzu die laufend aktualisierten Empfehlungen des BSI zu kryptografischen Verfahren in denen auch Angaben zur empfohlenen Schlüssellänge gemacht werden: BSI, TR-02102-1; siehe auch *Eckert*, IT-Sicherheit, 11. Aufl. 2023, S. 361; vgl. Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 17; vgl. auch *Hellmann*, IT-Sicherheit, 2. Aufl. 2023, S. 30, der darauf verweist, dass bei der Wahl der Schlüssellänge auf den zukünftigen Fortschritt zu achten ist.

<sup>142</sup> *Eckert*, IT-Sicherheit, 11. Aufl. 2023, S. 352; *Hellmann*, IT-Sicherheit, 2. Aufl. 2023, S. 30; Leupold/Wiebe/Glossner/*Leupold/Wiebe/Glossner*, IT-Recht, 4. Auflage 2021, Begriffserklärungen, Begriff „Brute-Force“; *Kroschwald*, ZD 2014, S. 75, 77; Kipker/*Sobr/Kemmerich*, Cybersecurity, 2. Aufl. 2023, Kapitel 3, Rn. 24.

<sup>143</sup> Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 34c f.; Taeger/Gabel/*Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 17; *Kroschwald*, ZD 2014, S. 75, 77; vgl. *Hellmann*, IT-Sicherheit, 2. Aufl. 2023, S. 30; siehe auch Kipker/*Sobr/Kemmerich*, Cybersecurity, 2. Aufl. 2023, Kapitel 3, Rn. 24, 29.

<sup>144</sup> Vgl. Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 79; siehe in eine ähnliche Richtung Auernhammer/*Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-

Abhängig davon, wie eng die Vorgaben des Gesetzgebers an die zu treffenden Maßnahmen wären, könnte es aufgrund späterer Entwicklungen dazu führen, dass die – vom Gesetzgeber gestellten Vorgaben – bereits nicht mehr in der Lage wären, das gewünschte Ziel zu erreichen, weil sie in der Praxis durch effektivere Maßnahmen ersetzt wurden oder wirkungslos geworden sind. Rechtlich würde der Gesetzgeber aber weiterhin die Implementierung der Maßnahmen an diese Vorgaben binden.

Um dem Normzweck nicht entgegenzustehen, müsste der Gesetzgeber entweder laufend die Vorgaben anpassen,<sup>145</sup> was hier bedeuten würde, die Datenschutz-Grundverordnung zu ändern.<sup>146</sup> Damit würde der Gesetzgeber dem (technischen) Fortschritt allerdings stets hinterherlaufen.

Je konkreter die Vorgaben sind, desto höher ist die Gefahr, dass diese Vorgaben mit der Zeit in Widerspruch zum Normzweck stehen können, weil sie nicht mehr geeignet sind, den ihr zugeordneten Schutz zu gewährleisten. Bei allgemeineren Vorgaben an die Maßnahmen ist diese Gefahr niedriger. Dies zeigt sich auch anhand des Art. 32 Abs. 1 Hs. 2 lit. a) DS-GVO. Dort werden schließlich Maßnahmen vom Gesetzgeber „vorgegeben“. Dies erfolgt mit der Pseudonymisierung und Verschlüsselung allerdings anhand eines Konzepts in Form von Maßnahmenkategorien und weniger anhand der später konkret umzusetzenden Weise, wie dieses Konzept zu etablieren ist, bspw. durch Vorgabe bestimmter

---

GVO, Rn. 18, die einmal darauf hinweisen, dass ein konkreter Maßnahmenkatalog sich den ändernden Gegebenheiten anpassen müsste und verweisen darauf, dass der Gesetzgeber dafür „gegenwärtig keine Verantwortung übernehmen will“ und lassen ebenfalls erkennen, dass ein solcher Katalog sehr umfangreich wäre. Siehe auch allgemein zum Problem des technischen Fortschritts für den Gesetzgeber bei der Gesetzgebung Kipker/*Ekrot/Fischer*, Cybersecurity, 2. Aufl. 2023, Kapitel 4, Vor. Rn. 1 und daher dem Erfordernis auf unbestimmte Rechtsbegriffe (hier dem Tatbestand „Stand der Technik“ (allgemein und nicht auf Art. 32 DS-GVO beschränkt)) zurückzugreifen (zudem mit Verweis auf BVerfGE 49, S. 89, 134 f.).

<sup>145</sup> Siehe bereits zu diesem Problem BVerfGE 49, S. 89, 134 f.; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 79, spricht im Zusammenhang von Art. 32 DS-GVO aufgrund der abstrakteren Vorgaben auch von einer zu erwartenden „längere[n] Lebensdauer“.

<sup>146</sup> Die EU-Kommission sprach sich in ihrem Entwurf noch die Befugnis zu, mittels delegierter Rechtsakte u.a. die Kriterien und Bedingungen für die technischen und organisatorischen Maßnahmen zu bestimmen, vgl. Art. 30 DS-GVO E (Kommission), KOM(2012) 11 endgültig. Dieses, im Vergleich zur Änderung der Datenschutz-Grundverordnung, weniger aufwendige Instrument konnte sich im Gesetzgebungsverfahren aber nicht durchsetzen, vgl. Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 20.

Verschlüsselungsverfahren. Solange nicht das ganze Sicherheitskonzept von Maßnahmen an Wirksamkeit verliert, besteht hier zumindest nicht die Gefahr, dass die gesamte Vorgabe im Widerspruch zum Schutzzweck steht.

Ein Widerspruch zwischen den rechtlichen Vorgaben und den verfolgten Zielen ließe sich damit aber dennoch nicht vollständig verhindern.

### *2. Vorgaben unter Berücksichtigung der Einzelfallprüfung*

Weiterhin muss beachtet werden, dass die Pflicht in der Gewährleistung eines *angemessenen* Schutzniveaus liegt. Wie gezeigt, ist die Angemessenheit des Schutzniveaus aber von verschiedenen Kriterien abhängig und bedarf erst einer genauen Bestimmung anhand des Einzelfalls. Vorgaben des Gesetzgeber bei den (später einzuführenden) technischen und organisatorischen Maßnahmen müssten dies berücksichtigen. Der Gesetzgeber kann nicht bestimmte Maßnahmen oder auch nur Maßnahmenkonzepte vorschreiben, die nicht gleichzeitig im Rahmen dessen liegen, wozu der Datenverarbeiter unter Abwägung der Verhältnismäßigkeit verpflichtet ist. Diese Pflicht muss im Rahmen des Art. 32 Abs. 1, 2 DS-GVO aber zunächst konkretisiert werden. Das macht es aber für den Gesetzgeber nahezu unmöglich, ein System aus Vorgaben festzulegen, das die unterschiedlichen Eventualitäten, die sich bei der Bestimmung des Schutzniveaus ergeben könnten, berücksichtigen kann.

### *3. Zielorientierte Pflicht*

Als letzten Punkt verdient ein Argument Beachtung, das bereits zuvor angesprochen wurde, aber in diesem Kontext noch einmal kurz in Erinnerung gerufen werden soll: Die Maßnahmen stellen lediglich das Mittel zum Zweck dar.<sup>147</sup> Ziel der Vorschrift ist die Gewährleistung des angemessenen Schutzniveaus. Dieses rechtliche Ziel soll auf faktischer Ebene mit der Implementierung technischer und organisatorischer Maßnahmen erreicht werden.

Welche Maßnahmen letztlich implementiert werden, seien es technische oder organisatorische Maßnahmen, wie sie im Einzelnen funktionieren oder auf welche Art und Weise sie das geforderte, angemessene Schutzniveau gewährleisten, ist für Art. 32 DS-GVO nebensächlich. Datenverarbeiter dürften daher auch grds. nach den finanziell günstigsten Maßnahmen suchen, sofern sie damit das angemessene Schutzniveau erreichen. Werden durch die implementierten

---

<sup>147</sup> Siehe hierzu bereits: Kap. 5, C., III., 2. *Maßnahmen als Mittel zum Zweck*.

Maßnahmen die Anforderungen an das Schutzniveau jedoch nicht erreicht, wird auch die Pflicht nach Art. 32 DS-GVO nicht erfüllt und es müssen andere oder zusätzliche Maßnahmen getroffen werden. Wie das angemessene Schutzniveau daher von Datenverarbeitern umzusetzen ist, obliegt ihrer Entscheidung.<sup>148</sup> Die Vorschrift ist damit zielorientiert gestaltet.<sup>149</sup>

### *VI. Zwischenergebnis*

Die technischen und organisatorischen Maßnahmen dienen als Mittel zur Umsetzung des angemessenen Schutzniveaus. Dabei ist nicht nur der Begriff der Maßnahmen sehr weit gefasst. Die Datenschutz-Grundverordnung stellt ferner auch keine nennenswerten Vorgaben an diese Maßnahmen. Dies dürfte vor allem daran liegen, dass Art. 32 DS-GVO mit der Anknüpfung an das angemessene Schutzniveau zielorientiert ausgestaltet ist. Für den Gesetzgeber dürfte daher im Fokus gestanden haben, dass das entsprechende Schutzniveau gewährleistet wird. Die Art und Weise, wie dieses letztlich umgesetzt wird, bleibt grds. den Verpflichteten überlassen.

Gesetzliche Vorgaben an die Maßnahmen könnten dabei sogar dem Regelungsziel schaden, wenn sie aufgrund technologischer Entwicklungen oder Zeitablauf ihren zugedachten Aufgaben nicht mehr gerecht werden können. Daher sollten die „Vorgaben“, mit denen Art. 32 DS-GVO die Umsetzung des angemessenen Schutzniveaus näher konkretisiert auch allenfalls als Orientierungshilfe angesehen werden, um den Zielen des Art. 32 DS-GVO nicht zu schaden.

---

<sup>148</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 31; Schuster/Grützmacher/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 26; Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 15; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 38, wobei im Einzelfall aber auch eine Pflicht bestehen kann, bestimmte Maßnahmen zu ergreifen.

<sup>149</sup> Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 78; vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 31; v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 15.

## Kapitel 6

### Wesentliche Ergebnisse für die Problemstellung

Aus der bisherigen Analyse des Art. 32 DS-GVO lassen sich einige wesentliche Ergebnisse für das Problem datenverarbeitender TOM dieser Arbeit herausarbeiten.

#### A. Der Regelungsinhalt von Art. 32 DS-GVO unter Beachtung des Problems datenverarbeitender TOM

##### *I. Pflicht zur Gewährleistung eines angemessenen Schutzniveaus*

Art. 32 DS-GVO regelt die Anforderungen an die Sicherheit der Verarbeitung anhand einer Einzelfallprüfung. Es gibt somit keine allgemeingültigen Anforderungen an die Sicherheit, die von allen Datenverarbeitern gleichermaßen einzuhalten sind. Vielmehr ist Ausgangspunkt das individuelle Risiko für die Rechte und Freiheiten der von der jeweiligen Verarbeitung betroffenen Person.<sup>1</sup>

Aus diesem Grund ist es von so herausragender Bedeutung, das Regelungsziel von Art. 32 DS-GVO zu kennen. Denn nur ein Verständnis hierüber macht die geforderte Risikobewertung möglich. Problematisch ist in diesem Zusammenhang, dass das Regelungsziel des Art. 32 DS-GVO aus der Verordnung nur nach einer näheren Analyse hervorgeht.<sup>2</sup> So kommt man zu dem Schluss, dass das Risiko für die Rechte und Freiheiten betroffener Personen während der Verarbeitung ihrer personenbezogenen Daten durch die Gefahren eines auftretenden

---

<sup>1</sup> Siehe hierzu: Kap. 5, A. *Risikobewertung*, Kap. 4, B. *Schutz der Rechte und Freiheiten* und Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>2</sup> Siehe hierzu: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO*.

den personal data breach begründet werden. Art. 32 DS-GVO möchte die betroffenen Personen also vor den Gefahren eines solchen personal data breach schützen.<sup>3</sup>

Die Anforderungen an die Sicherheit der Verarbeitung werden aber nicht einzig durch das Risiko eines personal data breach bestimmt. Die Verordnung stellt auf ein angemessenes Schutzniveau ab und verlangt daher eine Abwägung, um dem Gebot der Verhältnismäßigkeit gerecht zu werden.<sup>4</sup> Auch hier zeigen sich wieder technische Schwächen in der Vorschrift, da Art. 32 DS-GVO die Abwägungskriterien innerhalb der Vorschrift „versteckt“, was das Verständnis der Norm erheblich erschwert.<sup>5</sup> Nach entsprechender Auslegung sind neben dem Risiko für die Rechte und Freiheiten betroffener Personen auch der Stand der Technik, die Implementierungskosten und verarbeitungsbezogene Kriterien für die Angemessenheit des Schutzniveaus zu berücksichtigen.<sup>6</sup>

## II. Keine Pflicht zur Implementierung (datenverarbeitender) TOM

Für das Problem datenverarbeitender TOM von größerem Interesse dürfte jedoch der dritte Schritt bei der Gewährleistung der Sicherheit der Verarbeitung sein. Das – im Rahmen der ersten beiden Schritte (Risikobewertung und Angemessenheitsprüfung) – geforderte Schutzniveau ist anschließend durch technische und organisatorische Maßnahmen umzusetzen. Bei der Umsetzung ist zu beachten, dass Art. 32 DS-GVO keine „wirklichen“ Vorgaben an die Implementierung dieser technischen und organisatorischen Maßnahmen stellt.

Die einzigen „Vorgaben“ die sich in Art. 32 DS-GVO hierzu finden, können allenfalls als Orientierungshilfen angesehen werden. Denn ihr Inhalt lässt sich bereits allgemein aus der Pflicht zur Gewährleistung der Sicherheit der Verarbeitung ableiten.<sup>7</sup> Dabei ist zu berücksichtigen, dass Art. 32 DS-GVO zielorientiert ausgerichtet ist. Das bedeutet, dass die Pflicht zur Gewährleistung eines ange-

<sup>3</sup> Siehe hierzu: Kap. 4, C. Personal data breaches (und andere Sicherheitsvorfälle).

<sup>4</sup> Siehe hierzu: Kap. 5, B., I. Bedeutung der Angemessenheit.

<sup>5</sup> Siehe hierzu: Kap. 5, B., III. Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?

<sup>6</sup> Siehe hierzu: Kap. 5, B., III. Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?

<sup>7</sup> Siehe hierzu ausführlicher: Kap. 5, C., III. Geeignetheit der Maßnahmen und Kap. 5, C., IV. Anforderungen an die Maßnahmen nach Art. 32 Abs. 1 Hs. 2 DS-GVO.



messenen Schutzniveaus im Mittelpunkt steht. Dieses Ziel ist zwar durch entsprechende Maßnahmen umzusetzen. Wie diese Umsetzung im Detail erfolgt, obliegt jedoch den Datenverarbeitern.

Ausgehend von diesen Erkenntnissen kommt man zu dem Schluss, dass Art. 32 DS-GVO keine Verpflichtung kennt, bestimmte technische und organisatorische Maßnahmen zu implementieren, geschweige denn bestimmte (datenverarbeitende) TOM zu implementieren.<sup>8</sup> Solange die, von den Datenverarbeitern getroffenen Maßnahmen im Stande sind, das geforderte Schutzniveau zu gewährleisten, reicht dies für die Erfüllung der Verpflichtungen aus.

## B. Abgleich der bisherigen Erkenntnisse mit der Arbeitshypothese

Ausgehend von der Arbeitshypothese im 1. Teil wird das Problem datenverarbeitender TOM darin gesehen, dass die Datenschutz-Grundverordnung im Rahmen der Sicherheit der Verarbeitung eine Verpflichtung zur Implementierung dieser TOM aussprechen könnte, die im Widerspruch zu den Voraussetzungen einer rechtmäßigen Datenverarbeitung nach Art. 6 DS-GVO steht. Art. 32 DS-GVO dürfte demnach die Implementierung datenverarbeitender TOM zur Gewährleistung der Sicherheit der Verarbeitung nicht fordern, wenn

---

<sup>8</sup> Siehe hierzu ausführlicher: Kap. 5, C. *Technische und organisatorische Maßnahmen*. Im Ergebnis auch *Gärtner/Selzer*, DuD 2023, S. 289, 290; *Johannes/Geminn*, InTeR 2021, S. 140, 141; *Gola/Heckmann/Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 3; vgl. EuGH, Rs. C-340/21 (*Natsionalna agentsia za prihodite*), ECLI:EU:C:2023:986 = BeckRS 2023, 35786, Rn. 43, der von einem „gewissen Ermessensspielraum bei der Festlegung“ spricht; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 31, „(Auswahl-)Ermessen“; *Auernhammer/Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 18 f., „Beurteilungsspielraum“; *Kipker/Reusch/Ritter/Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 38, sprechen ebenfalls von einem „Auswahlermessen“, dass sich allerdings „auf null reduzier[en]“ kann, mit der Folge, dass bestimmte Maßnahmen zu implementieren sind; ähnlich *Sundermann*, DuD 2021, S. 594, 594, der von einem „Spielraum“ bei der „Festlegung der Schutzmaßnahmen“ spricht, der entfällt, wenn eine „ganz bestimmte[...] Schutzmaßnahme von Rechts wegen verpflichte[nd] ist“, was jedoch den Ausnahmefall darstellen sollte. Siehe noch ausführlicher sogleich: Kap. 6, C., I. „Pflicht“ zur Implementierung bestimmter (datenverarbeitender) TOM.

die datenschutzrechtliche Vorabkontrolle gleichzeitig die ihnen zugrundeliegende Datenverarbeitung „ablehnt“.<sup>9</sup>

Die Untersuchung von Art. 32 DS-GVO hat nun gezeigt, dass die Vorschrift keine (nennenswerten) Vorgaben an die Implementierung bestimmter TOM stellt. Datenverarbeiter werden daher nach Art. 32 DS-GVO nicht unmittelbar dazu verpflichtet, bestimmte (datenverarbeitende) TOM zu implementieren. Im Fokus der Vorschrift steht einzig die Gewährleistung des angemessenen Schutzniveaus und somit das zu erreichende Ziel. Wie dieses Ziel erreicht wird, also mit welchen Maßnahmen das angemessene Schutzniveau gewährleistet wird, liegt in der Entscheidung der Datenverarbeiter. Entscheidet sich der Datenverarbeiter bei der Gewährleistung des angemessenen Schutzniveaus für die Implementierung datenverarbeitender TOM, läge es demnach in seiner Verantwortung zu überprüfen, ob die, den TOM zugrundeliegende Datenverarbeitung im Einklang mit den Anforderungen an die datenschutzrechtliche Vorabkontrolle i.S.d. Art. 6 DS-GVO steht. Sollte dies nicht der Fall sein, darf der Datenverarbeiter diese TOM zwar weiterhin nicht implementieren. Nach Art. 32 DS-GVO wäre er aber dann nur dazu verpflichtet, das angemessene Schutzniveau mit anderen Maßnahmen zu gewährleisten.

Aufgrund dieser zielorientierten Regelungstechnik des Art. 32 DS-GVO fehlt es an einem unmittelbaren Widerspruch zwischen Art. 32 DS-GVO und Art. 6 DS-GVO. Denn rein rechtlich betrachtet wird von den Datenverarbeitern nicht die Implementierung bestimmter TOM verlangt, die dann an anderer Stelle der Rechtsordnung verboten sein könnten. Daher könnte man zu der Auffassung kommen, dass der Konflikt im Rahmen datenverarbeitender TOM, wie er noch im 1. Teil dieser Arbeit beschrieben wurde, so nicht besteht. Selbst wenn man dieser Auffassung folgen würde, ändert dies aber nichts daran, dass datenverarbeitende TOM weiterhin in einem Spannungsverhältnis zwischen Art. 32 DS-GVO und Art. 6 DS-GVO stehen. Denn Datenverarbeiter hätten weiterhin bei der Gewährleistung der Sicherheit der Verarbeitung mittels datenverarbeitender TOM die Anforderungen nach Art. 6 DS-GVO zu beachten. Ob dieses Spannungsverhältnis damit gelöst werden kann, dass Datenverarbeiter bei einer unzulässigen Datenverarbeitung durch datenverarbeitende TOM darauf verwiesen werden können, die Sicherheit der Verarbeitung mit anderen Maßnahmen zu gewährleisten, muss jedoch nachfolgend geklärt werden.

---

<sup>9</sup> Siehe hierzu: Kap. 2, A. Begründung eines Spannungsverhältnisses zwischen Art. 32 und Art. 6 DS-GVO.

## C. Überarbeitung der Arbeitshypothese

Eine rechtliche Pflicht zur Implementierung bestimmter, vor allem datenverarbeitender, TOM ergibt sich nicht unmittelbar aus Art. 32 DS-GVO. Dies kann aber nicht bedeuten, dass es bei datenverarbeitenden TOM kein Spannungsverhältnis zwischen Art. 32 DS-GVO und den Anforderungen nach Art. 6 DS-GVO gäbe und das Problem dieser TOM damit gelöst sei.

### I. „Pflicht“ zur Implementierung bestimmter (datenverarbeitender) TOM

Begründet Art. 32 DS-GVO keine unmittelbare (rechtliche) Pflicht zur Implementierung bestimmter (datenverarbeitender) Maßnahmen, so kann sich eine solche „Pflicht“ aus tatsächlichen Umständen ergeben.

#### 1. „Zwingende“ Maßnahmen für die Gewährleistung des angemessenen Schutzniveaus

Kann das angemessene Schutzniveau bspw. nur mit einer bestimmten Maßnahme erreicht werden, dann schränkt sich die – nach Art. 32 DS-GVO ergebene – Freiheit des Datenverarbeiters bei der Auswahl der Maßnahmen faktisch ein.<sup>10</sup> In diesem Fall muss die (bestimmte) Maßnahme implementiert werden, um dem geforderten Schutzniveau und damit den Anforderungen an die Sicherheit der Verarbeitung gerecht zu werden. Es entsteht eine faktische „Pflicht“ zur Implementierung. Handelt es sich dann noch um eine datenverarbeitende Maßnahme, begründet dies gleichzeitig den Konflikt mit der datenschutzrechtlichen Vorabkontrolle.

Nun wurde bereits darauf aufmerksam gemacht, dass das angemessene Schutzniveau in den wenigsten Fällen durch einzelne Maßnahmen gewährleistet werden kann, da sich das Schutzniveau auf die gesamte Verarbeitung bezieht.<sup>11</sup> Dabei dürften die Gefahren eines personal data breach, über die Verarbeitung

---

<sup>10</sup> Hierauf verweisen wohl auch Kipker/Reusch/Ritter/Piltz/Zwerschke, *Recht der Informationssicherheit*, 2023, *Datenschutz-Grundverordnung*, Art. 32 DS-GVO, Rn. 38, mit dem Hinweis, dass sich das „Auswahlermessen“ „auf null reduzier[en]“ kann und dann ganz bestimmte Maßnahmen zu implementieren sind.

<sup>11</sup> Siehe hierzu: Kap. 5, A. *Risikobewertung*.

verteilt, vielfältig sein und sich nicht mit einzelnen Maßnahmen adressieren lassen.<sup>12</sup> Auch wenn das (gesamte) angemessene Schutzniveau nicht mit einer einzelnen Maßnahme gewährleistet werden kann, heißt das jedoch nicht, dass nicht einzelne Maßnahmen darüber entscheiden können, ob das geforderte Schutzniveau nun erreicht wurde oder nicht. Denn selbst bei einem ganzen Maßnahmenpaket könnten einzelne Maßnahmen bestehen, deren Beitrag zwingend für die Gewährleistung des angemessenen Schutzniveaus sind und die sich ggf. nicht durch andere Maßnahmen austauschen lassen.<sup>13</sup>

## 2. Datenverarbeitende TOM als zwingende Maßnahmengruppe

Doch selbst wenn man die Annahme verträte, die Abhängigkeit der Sicherheit der Verarbeitung von ganz bestimmten Maßnahmen, stelle den absoluten Ausnahmefall dar, kann den Konflikt bei datenverarbeitenden TOM nicht widerlegen. Denn der Konflikt bei datenverarbeitenden TOM zeigt sich nicht erst, wenn die Sicherheit der Verarbeitung nur durch eine ganz bestimmte Maßnahme erreicht werden kann.

Es reicht bereits aus, wenn die Sicherheit der Verarbeitung von einer bestimmten Maßnahmengruppe, also datenverarbeitender TOM, abhängt. Dies ist der Fall, wenn die Sicherheit der Verarbeitung zwar auf verschiedene Weise gewährleistet werden kann, aber jede dieser Umsetzungen die Implementierung von (unterschiedlichen) datenverarbeitenden TOM voraussetzt. Damit besteht

---

<sup>12</sup> Siehe Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 27, der eine „Kombination mehrerer Maßnahmen“ für die Umsetzung der Ziele nach Art. 32 Abs. 1 lit. b) und c) DS-GVO i.d.R. für erforderlich hält. Vgl. auch Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 46, wonach generell bei der Umsetzung eines Schutzziels (der IT-Sicherheit) meist mehrere Maßnahmen erforderlich sind; siehe auch ähnlich und unmittelbar zu Art. 32 DS-GVO Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 5; ähnlich und auch konkret zu Art. 32 DS-GVO Gärtner/Selzer, DuD 2023, S. 289, 290, wonach „häufig mehrere Maßnahmen zusammenwirken, um eines der Datensicherheitsziele umzusetzen“.

<sup>13</sup> Vgl. auch Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 38, mit dem Verweis auf ein „Auswahlermessen“, dass sich allerdings „auf null reduzier[en]“ kann, mit der Folge, dass bestimmte Maßnahmen zu implementieren sind; siehe auch Sundermann, DuD 2021, S. 594, 594, der von einem „Spielraum“ bei der „Festlegung der Schutzmaßnahmen“ spricht, der entfällt, wenn eine „ganz bestimmte[...] Schutzmaßnahme von Rechts wegen verpflichte[nd] ist“, was jedoch den Ausnahmefall darstellen sollte.

keine faktische „Pflicht“ zur Implementierung einer bestimmten Maßnahme. In jedem Fall verlangt aber die Gewährleistung des angemessenen Schutzniveaus die Verarbeitung personenbezogener Daten durch die Implementierung irgend-einer dieser datenverarbeitenden TOM. Und diese Datenverarbeitung ist der ausschlaggebende Punkt für den Konflikt.

Berücksichtigt man hierbei die Entwicklungen der Digitalisierung, dürften datenverarbeitende TOM von ihrer Zahl und Bedeutung weiter zunehmen, während „herkömmliche“ Maßnahmen wohl in den Hintergrund treten.<sup>14</sup> Damit erhöht sich aber auch die Gefahr, dass die Sicherheit der Verarbeitung von der Implementierung datenverarbeitender TOM abhängen kann und somit den dargestellten Konflikt begründet.

## II. Anordnung von Sicherheitsmaßnahmen durch Aufsichtsbehörden

Ein anderer Fall, in dem sogar eine rechtliche Pflicht zur Implementierung bestimmter Maßnahmen besteht, ist die Anordnung durch eine Aufsichtsbehörde. Aufsichtsbehörden haben nach Art. 58 Abs. 2 lit. d) DS-GVO die Befugnis, Verantwortliche und Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge auf bestimmte Weise in Einklang mit der Datenschutz-Grundverordnung zu bringen. Hiervon umfasst ist auch die Anordnung, Maßnahmen zur Gewährleistung der Sicherheit zu ergreifen.<sup>15</sup> Es handelt sich hierbei zwar nicht um eine Pflicht, die unmittelbar aus Art. 32 DS-GVO erwächst. Als bindender Verwaltungsakt<sup>16</sup> müssten Datenverarbeiter einer solchen Aufforderung jedoch nachkommen und die geforderten Maßnahmen ergreifen oder die Wirksamkeit des Verwaltungsakts bspw. im Sinne einer „Anfechtungsklage“ (vgl. Art. 78

---

<sup>14</sup> Siehe zur Bedeutung datenverarbeitender TOM bereits allgemein und anhand von Beispielen: Kap. 2, C. *Die Bedeutung datenverarbeitender TOM*.

<sup>15</sup> Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 125; Simitis/Hornung/Spiecker gen. Döhmann/Polenz, Datenschutzrecht, 2019, Art. 58 DS-GVO, Rn. 33; Paal/Pauly/Körffler, DS-GVO BDSG, 3. Aufl. 2021, Art. 58 DS-GVO, Rn. 20; vgl. Ehmann/Selmayr/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 58 DS-GVO, Rn. 22.

<sup>16</sup> Vgl. zur Einordnung als Verwaltungsakt: BeckOK Datenschutzrecht/Eichler/Matzke, Stand: 46. Ed. 2023, Art. 58 DS-GVO (Stand: August 2023), Rn. 25; Gola/Heckmann/Nguyen, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 58 DS-GVO, Rn. 16; Plath/Hullen, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 58 DS-GVO, Rn. 12; siehe auch Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 1100 f.; Jandt/Steidle/Ambrock, Datenschutz im Internet, 2018, B. VII., Rn. 28.

Abs. 1 DS-GVO) angreifen.<sup>17</sup> Es kommt insofern auch zu einer Pflicht zur Implementierung bestimmter Maßnahmen und kann zu dem beschriebenen Konflikt bei datenverarbeitenden TOM führen. Da diese Pflicht keine direkte Folge des Art. 32 DS-GVO ist, sollte dieser Fall der Vollständigkeit halber kurz aufgezeigt aber im weiteren Verlauf nicht weiter behandelt werden.

### *III. Gefahr einer Verzerrung der Angemessenheit*

In den Fällen, in denen eine (faktische) „Pflicht“ zur Implementierung datenverarbeitender TOM besteht und zur Gewährleistung der Sicherheit der Verarbeitung Maßnahmen gefordert werden, deren zugrundeliegende Datenverarbeitung aus Sicht der datenschutzrechtlichen Vorabkontrolle i.S.d. Art. 6 DS-GVO jedoch rechtlich bedenklich sein könnten, wird aus dem Spannungsverhältnis ein echter Konflikt.

Wird (nachträglich) die Implementierung bestimmter Sicherheitsmaßnahmen „verboten“, tangiert dies die Auswahlfreiheit der Datenverarbeiter bei der Umsetzung des angemessenen Schutzniveaus. Nun könnte man zwar argumentieren, dass – solange andere Maßnahmen zur Verfügung stünden – es den Datenverarbeitern weiterhin möglich wäre, die gebotenen Anforderungen an die Sicherheit der Verarbeitung zu erfüllen. Die verbleibenden Möglichkeiten könnten aber im Widerspruch zu dem zugrundeliegenden Gebot der Verhältnismäßigkeit<sup>18</sup> stehen.

Denn leitet man das geforderte Schutzniveau auf Grund des Gebots der Verhältnismäßigkeit erst aus einer Angemessenheitsprüfung ab – bei der man sich wohl zwangsweise Gedanken über die spätere Umsetzung dieses Schutzniveaus machen müsste – und „entfernt“ dann in einem nächsten Schritt wieder einzelne Maßnahmen aus diesen Überlegungen, kann sich dies auf die zuvor bestimmte Angemessenheit des Schutzniveaus durchschlagen. Denn dem zuvor

---

<sup>17</sup> Siehe zur Ausübung des Rechts nach Art. 78 Abs. 1 DS-GVO insb. gegen Maßnahmen nach Art. 58 Abs. 2 DS-GVO im Wege der, nach deutschem Recht, „Anfechtungsklage“: Sydow/Marsch/Sydow, DS-GVO – BDSG, 3. Aufl. 2022, Art. 78 DS-GVO, Rn. 20 ff.; auch Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 1100 ff.

<sup>18</sup> Das Art. 32 DS-GVO diesem folgt: Statt vieler Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 9; siehe bereits: Kap. 5, B., I. *Bedeutung der Angemessenheit*.

bestimmten Schutzniveau liegt noch die Annahme zugrunde, dass alle verhältnismäßigen Maßnahmen zur Verfügung stünden, obwohl dieser Pool nachträglich verkleinert wird.

Um dem Gebot der Verhältnismäßigkeit gerecht zu werden, müsste man daher bereits bei der Bestimmung der Angemessenheit des Schutzniveaus berücksichtigen, dass der späteren Umsetzung ggf. rechtliche Hindernisse entgegenstehen könnten, wenn bspw. einzelne Sicherheitsmaßnahmen aufgrund einer etwaigen (rechtswidrigen) Datenverarbeitung nicht als Mittel zur Gewährleistung des Schutzes eingesetzt werden können. Andernfalls käme es zu einer Verzerrung der Angemessenheitsprüfung, da diese ggf. unter verfälschten Kriterien erfolgt.

## D. Schlussfolgerung

Auch wenn die Sicherheit der Verarbeitung keine rechtlichen Pflichten an die Implementierung von TOM kennt und den Datenverarbeitern die Freiheit einräumt die Maßnahmen zur Gewährleistung des angemessenen Schutzniveaus zu wählen, kann hieraus nicht gefolgert werden, dass ein Konflikt mit der datenschutzrechtlichen Vorabkontrolle nicht besteht. „Pflichten“ zur Implementierung bestimmter (datenverarbeitender) Maßnahmen können sich faktisch ergeben, wenn die Sicherheit der Verarbeitung ohne den Einsatz dieser Maßnahmen nicht gewährleistet werden kann.

Zudem lässt sich ein allgemeines Spannungsverhältnis identifizieren, da ein mögliches „Verbot“ einzelner Sicherheitsmaßnahmen auf die Prüfung der Angemessenheit des Schutzniveaus durchschlagen und zu einer Verzerrung der Angemessenheit führen kann. Im Vergleich zu ersterem dürfte diese Verzerrung zwar in ihren Folgen nicht so stark ausgeprägt sein, da weiterhin die Möglichkeit bestünde, die Sicherheit der Verarbeitung auf andere Weise zu gewährleisten. Dennoch tangiert sie das zugrundeliegende Gebot der Verhältnismäßigkeit und dürfte sich damit auf ein wesentliches Prinzip der Sicherheit der Verarbeitung auswirken.

Zwar wurden zuvor bereits einige grundlegenden Aspekte dieser Angemessenheitsprüfung dargestellt. Für die weitere Lösung dürfte dies hingegen nicht ausreichen. Es bedarf eines besseren systematischen Verständnisses darüber, wo und wie Art. 32 DS-GVO die Grenzen für die Sicherheit der Verarbeitung zieht

und in diesem Zusammenhang vor allem, wie sich dabei das Gebot der Verhältnismäßigkeit auswirkt.



## Kapitel 7

# Berücksichtigung datenverarbeitender TOM

### A. Überlegungen zur Berücksichtigung datenverarbeitender TOM

Das vorherige Kapitel hat gezeigt, dass Art. 32 DS-GVO zwar keine Anforderungen an die Implementierung bestimmter Sicherheitsmaßnahmen stellt und damit auch keine Pflicht zur Implementierung datenverarbeitender TOM kennt. Dennoch besteht ein Spannungsverhältnis zwischen Art. 32 DS-GVO und den Vorschriften zur datenschutzrechtlichen Vorabkontrolle nach Art. 6 DS-GVO bei datenverarbeitenden TOM, da sie auf das angemessene Schutzniveau und damit die Sicherheit der Verarbeitung allgemein durchschlagen können. Dabei gilt es einige grundlegende Punkte zu beachten.

#### *I. Zwingende Differenzierung zwischen Sicherheit und Sicherheitsmaßnahmen*

Ein wesentlicher Punkt, den es für die Lösung des Problems datenverarbeitender TOM auf Seiten der Sicherheit der Verarbeitung zu beachten gilt, ist die zwingende Differenzierung zwischen der Sicherheit der Verarbeitung im Allgemeinen und den Sicherheitsmaßnahmen selbst. Wie bereits mehrfach darauf hingewiesen wurde, dienen die (Sicherheits-)Maßnahmen der Umsetzung des angemessenen Schutzniveaus und damit der Sicherheit der Verarbeitung. Nur an letzteres stellt die Verordnung in Art. 32 DS-GVO gesonderte Anforderungen.

Die Sicherheit umfasst die gesamte Datenverarbeitung<sup>1</sup> und gibt ein bestimmtes Niveau vor, das anschließend mittels technischer und organisatorischer Maßnahmen zu gewährleisten ist. Die Maßnahmen sind folglich nur Mittel zum Zweck. Es wird in der Praxis selten vorkommen, dass das geforderte

---

<sup>1</sup> Siehe bereits: Kap. 5, A. *Risikobewertung*.

Schutzniveau mit einer einzigen Maßnahme erreicht werden kann.<sup>2</sup> Vielmehr bedarf es wohl einer Vielzahl an Maßnahmen, die die identifizierten Gefahren angemessen adressieren. Gleichzeitig wird es wohl oftmals mehrere Maßnahmen geben, die eine bestehende Gefahr adressieren können.<sup>3</sup> Eine Pflicht zur Gewährleistung der Sicherheit der Verarbeitung ist damit nicht gleichzusetzen mit der Pflicht zu Implementierung (bestimmter) technischer und organisatorischer Maßnahmen.

Für eine Lösung des Problems datenverarbeitender TOM bedeutet dies, dass einzelne Sicherheitsmaßnahmen in den meisten Fällen nicht über die Gewährleistung der Sicherheit der Verarbeitung entscheiden. Der Regelfall sieht eher so aus, dass den Datenverarbeitern eine Bandbreite von Maßnahmen zur Verfügung steht, die Sicherheit der Verarbeitung zu gewährleisten und auch einzelne Gefahren zu adressieren. Ein Wegfall einzelner Sicherheitsmaßnahmen, bspw. weil deren Implementierung rechtlich verboten ist, muss damit in seinen Auswirkungen an die Regelungssystematik des Art. 32 DS-GVO angepasst werden.

## II. Datenverarbeitende TOM als Teil der Angemessenheitsprüfung

Mit Blick auf Art. 32 DS-GVO kann eine Lösung datenverarbeitender TOM damit nicht auf der Ebene der einzelnen Sicherheitsmaßnahmen gefunden werden. Um nämlich den Anforderungen an die Sicherheit der Verarbeitung gerecht werden zu können, muss an den Regelungsinstrumenten des Art. 32 DS-GVO angeknüpft werden. Die Berücksichtigung datenverarbeitender TOM muss daher am Schutzniveau ansetzen bzw. konkret bei dessen Angemessenheit. Um den aufgezeigten Problemen zu begegnen, muss auf Seiten der Sicherheit der Verarbeitung das Schutzniveau so weit herabgesenkt werden, dass dieses mittelbar nicht zur Implementierung unzulässiger Sicherheitsmaßnahmen verpflichten kann. Weiterhin muss das Gebot der Verhältnismäßigkeit beachtet werden. Denn nachgelagerte, bei der Angemessenheit noch nicht berücksichtigte Einschränkungen bei der Implementierung der TOM könnten ansonsten die Angemessenheit zu einer fiktiven Abwägung verkommen lassen.

---

<sup>2</sup> Vgl. bereits: Kap. 6, C., I., 1. „Zwingende“ Maßnahmen für die Gewährleistung des angemessenen Schutzniveaus.

<sup>3</sup> Vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 8, aber wohl eher auf das Gesamtrisiko bezogen. Siehe auch Schuster/Grützmacher/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 26, der gerade bei „alternativen Maßnahmen“ ein Auswahlermessens zuspricht.

Aufgrund der notwendigen Differenzierung zwischen der Sicherheit insgesamt und den einzelnen Maßnahmen, die diese gewährleisten sollen, können dabei Wertungen über einzelne Maßnahmen nicht unmittelbar auf die gesamte Sicherheit übertragen werden. Nur weil einzelne Sicherheitsmaßnahmen nicht implementiert werden können, heißt das noch nicht, dass gleich das geforderte Schutzniveau abgesenkt werden muss. Gleichzeitig darf ein (rechtliches) Verbot zur Implementierung einzelner Sicherheitsmaßnahmen aber auch nicht vollkommen unberücksichtigt für das zu fordernde Schutzniveau bleiben.

Im Rahmen der Angemessenheitsprüfung könnte diesem Umstand aber unter Berücksichtigung beider Aspekte Rechnung getragen werden, da es dann zu einer Abwägung mit den (anderen) Abwägungskriterien käme. Dem Verbot käme damit weder eine absolute Geltung zu, noch würde man es gänzlich unberücksichtigt lassen. Vielmehr würden man diesen Aspekt in das System des Art. 32 DS-GVO integrieren.

### *III. Die datenschutzrechtliche Bewertung von Sicherheitsmaßnahmen*

Zu klären bleibt damit nachfolgend, wie sich datenverarbeitende TOM innerhalb der Angemessenheitsprüfung berücksichtigen lassen könnten. Im Kern müsste es darum gehen, die rechtlichen Anforderungen an Sicherheitsmaßnahmen zum Teil der Angemessenheitsprüfung zu machen. Im Falle der datenverarbeitenden TOM sind dies die Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Sicherheitsmaßnahmen selbst, die durch die datenschutzrechtliche Vorabkontrolle vorgesehen werden.

Ein Lösungsansatz des Problems datenverarbeitender TOM im Rahmen des Art. 32 DS-GVO setzt demnach voraus, dass die datenschutzrechtliche Bewertung dieser TOM innerhalb der Angemessenheitsprüfung des Schutzniveaus berücksichtigt werden kann.<sup>4</sup> Ob und ggf. wie die datenschutzrechtliche Bewertung von TOM Einzug in die Angemessenheitsprüfung finden kann, erfordert eine nähere Untersuchung der Prüfung gem. Art. 32 DS-GVO und ihrer Kriterien.

---

<sup>4</sup>Die Möglichkeit, die Datenverarbeitung im Rahmen von TOM nach Art. 32 DS-GVO innerhalb des Grundsatzes der Verhältnismäßigkeit und demnach der Angemessenheitsprüfung zu berücksichtigen, spricht bereits *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 43 an, zieht aber wohl im Ergebnis eine Lösung über Art. 6 DS-GVO vor.

## B. Subsumtion unter die Abwägungskriterien des Art. 32 Abs. 1 DS-GVO

Datenverarbeitende TOM bzw. deren datenschutzrechtliche Bewertung ließen sich zunächst im Rahmen der Angemessenheitsprüfung berücksichtigen, wenn sie sich unter eines der Abwägungskriterien subsumieren lassen. Zur Erinnerung: Art. 32 Abs. 1 DS-GVO umfasst vier (Haupt-)Kriterien. Diese sind (1) der Stand der Technik, (2) die Implementierungskosten, (3) die „Verarbeitungskriterien“ und (4) das Risiko für die Rechte und Freiheiten natürlicher bzw. betroffener<sup>5</sup> Personen.

### I. Stand der Technik

Das erste Kriterium ist der „Stand der Technik“<sup>6</sup>. Der Stand der Technik bezieht sich auf die technischen und organisatorischen Maßnahmen.<sup>7</sup> Anders als eine mögliche, sprachliche Assoziation des deutschen Begriffs „Stand der Technik“<sup>8</sup> mit den „technischen Maßnahmen“ dies vielleicht suggerieren mag, beschränkt sich dieses Kriterium nicht nur auf solche Maßnahmen. Der „Stand der Technik“ umfasst auch organisatorische Maßnahmen.<sup>9</sup> Der englische und italienische Wortlaut drücken dies mit den Begriffen „state of the art“ bzw. „dello stato dell'arte“ klarer aus, denn sie verzichten auf die begriffliche Assoziationsmöglichkeit von „Technik“ mit „technischen Maßnahmen“.<sup>10</sup> Noch weiter geht die

<sup>5</sup> Siehe zur Eingrenzung, dass es sich vielmehr um das Risiko betroffener Personen handelt: Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>6</sup> Englisch: „state of the art“, Französisch: „de l'état des connaissances“, Spanisch: „el estado de la técnica“, Italienisch: „dello stato dell'arte“, Niederländisch: „stand van de techniek“.

<sup>7</sup> *Bartels/Backer*, DuD 2018, S. 214, 215, 216; *Johannes/Geminn*, InTeR 2021, S. 140, 143; vgl. *Knyrim/Pollirer*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.4; siehe auch *Taeger/Gabel/Lang*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 25 DS-GVO, Rn. 55, zum wortgleichen Begriff in Art. 25 DS-GVO.

<sup>8</sup> Vgl. auch Spanisch: „el estado de la técnica“, Niederländisch: „stand van de techniek“.

<sup>9</sup> *Bartels/Backer*, DuD 2018, S. 214, 216; *Sydow/Marsch/Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10, mit allgemeinem Verweis auf den wortgleichen Begriff in Art. 25 DS-GVO (siehe seine Kommentierung dort zu Art. 25 DS-GVO, Rn. 37); *EDSA*, Leitlinien 4/2019, Rn. 21, zu Art. 25 DS-GVO; *Taeger/Gabel/Lang*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 25 DS-GVO, Rn. 55, ebenfalls zu Art. 25 DS-GVO.

<sup>10</sup> Siehe auch *Gola/Heckmann/Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 17, im Vergleich mit dem englischen Begriff;

französische Sprachfassung, die wohl eher auf den Wissenstand oder Erkenntnisstand („*de l'état des connaissances*“) abstellt.

Bei dem Kriterium handelt es sich um einen Qualitätsstandard.<sup>11</sup> In der Literatur wird dabei das Kriterium in Abgrenzung zu den Begriffen „*Stand von Wissenschaft und Technik*“ und „*(allgemein anerkannte) Regeln der Technik*“ gesetzt.<sup>12</sup> Was allerdings konkret unter dem Stand der Technik zu verstehen ist, wird nicht legal definiert.<sup>13</sup> In der Diskussion werden Maßnahmen verbreitet dem Stand der Technik zugeordnet, wenn sie auf dem Markt verfügbar sind und

---

*Bartels/Backer*, DuD 2018, S. 214, 216, verweisen ebenfalls auf den „*neutraler[en]*“ englischen Begriff, um herauszustellen, dass auch organisatorische Maßnahmen erfasst sind.

<sup>11</sup> *Johannes/Geminn*, InTeR 2021, S. 140, 142; *Bartels/Backer*, DuD 2018, S. 214, 215; vgl. *Weidenhammer/Gundlach*, DuD 2018, S. 106, 106; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 10; siehe auch Taeger/Gabel/Lang, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 25 DS-GVO, Rn. 55, zum wortgleichen Begriff in Art. 25 DS-GVO.

<sup>12</sup> Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 10; *Johannes/Geminn*, InTeR 2021, S. 140, 142; *Gärtner/Selzer*, DuD 2023, S. 289, 291 f.; *Weidenhammer/Gundlach*, DuD 2018, S. 106, 106; Knyrim/Pollirer, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.5, spricht von „*Stand der Wissenschaft und Forschung*“, siehe aber auch DatKomm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 20 dort mit dem Verweis auf den „*Stand von Wissenschaft und Technik*“; ebenfalls vom „*Stand der Wissenschaft und Forschung*“ spricht Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 151; auch *Bartels/Backer*, DuD 2018, S. 214, 215; *Knopp*, DuD 2017, S. 663, 664, spricht auch vom „*Stand der Wissenschaft und Forschung*“, steht aber wohl insgesamt kritisch einer Heranziehung bei der Auslegung des Begriffs in der Datenschutz-Grundverordnung (S. 665) gegenüber. Siehe auch allgemein zu dieser Differenzierung bereits BVerfGE 49, S. 89, 135 f., auf die einige Stimmen aus der Literatur konkret verweisen.

<sup>13</sup> Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 14; *Johannes/Geminn*, InTeR 2021, S. 140, 142; *Gärtner/Selzer*, DuD 2023, S. 289, 291; vgl. Laue/Kremer/Laue, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7, Rn. 25, der allgemein auf eine fehlende Konkretisierung hinweist; *Knopp*, DuD 2017, S. 663, 665, der auf fehlende Erklärungen in den Erwägungsgründen verweist.

ihr effektiver Einsatz (hier zur Gewährleistung der Sicherheit)<sup>14</sup> bereits nachgewiesen wurde.<sup>15</sup> In Abgrenzung zum „Stand der Wissenschaft und Technik“ und den „(allgemein anerkannten) Regeln der Technik“ wird der „Stand der Technik“ als mittlerer Standard zwischen diesen beiden Standards eingeordnet.<sup>16</sup>

Ob Art. 32 DS-GVO mit dem Kriterium „Stand der Technik“ die Umsetzung der Sicherheit der Verarbeitung auf dieses oder überhaupt irgendein Niveau tatsächlich „begrenzen“ möchte und wie der Tatbestand im Detail auszu- liegt, liegt nicht im Fokus dieser Arbeit und bedarf daher grds. keiner abschließend Klärung. Allerdings steht die Auslegung des Begriffs teilweise im Zusammenhang mit der allgemeinen Funktion und den Zielen der Angemessenheitsprüfung und könnte auch für die hier untersuchte datenschutzrechtliche

---

<sup>14</sup> Hier ist erneut darauf hinzuweisen, dass technische und organisatorische Maßnahmen innerhalb der Datenschutz-Grundverordnung unterschiedliche Ziele verfolgen können, siehe hierzu bereits: Kap. 2, C., I. *Das Spannungsverhältnis bei datenverarbeitenden TOM in der aktuellen Diskussion*, insb. auch Fn. 33.

<sup>15</sup> Vgl. Ehmann/Selmayr/Hladjk, *Datenschutz-Grundverordnung*, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 5, „zur Verfügung stehen“ und „entsprechend bewährt haben“; ähnlich Laue/Kremer/Laue, *Das neue Datenschutzrecht in der betrieblichen Praxis*, 2. Aufl. 2019, § 7, Rn. 25; Kühling/Buchner/Jandt, *DS-GVO – BDSG*, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 10, „marktfähigen Techniken“ und „aktuell einen hohen Sicherheitsstandard aufweisen“; Gärtner/Selzer, *DuD* 2023, S. 289, 291, „praktische Eignung [...] unter Beweis gestellt worden sein“ und „technisch realisiert werden können“; Piltz, *K&R* 2016, S. 709, 714, „bekannte und bewährte Maßnahmen“, siehe aber dann Kipker/Reusch/Ritter/Piltz/Zwerschke, *Recht der Informationssicherheit*, 2023, *Datenschutz-Grundverordnung*, Art. 32 DS-GVO, Rn. 15, verweisen darauf, dass diese Maßnahmen „in der breiten Anwendung bekannt“ und „in der praktischen Anwendung bewährt“ sind, sprechen aber auch davon, dass es um Maßnahmen geht, die „am effektivsten [sind], um die [...] Ziele zu erreichen“, aber auch mit Verweis auf die gebotene europäische Auslegung und damit einer national geprägten Definition kritisch gegenüberstehen (Rn. 19); siehe auch Knopp, *DuD* 2017, S. 663, 664, spricht von „am Markt verfügbaren Bestleistungen“ und ebenfalls kritisch für die Auslegung der Datenschutz-Grundverordnung (S. 665); ähnlich Bartels/Backer, *DuD* 2018, S. 214, 215 f., gegen einen pauschalen Verweis auf nationales Recht aufgrund des Vorrangs des EU-Rechts und ebenfalls abstellend auf „am Markt verfügbare Bestleistung“. Siehe auch Weidenhammer/Gundlach, *DuD* 2018, S. 106, 107 ff. mit der Definition eigener Kriterien zur Bestimmung des Stands der Technik.

<sup>16</sup> Kühling/Buchner/Jandt, *DS-GVO – BDSG*, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 10; Paal/Pauly/Martini, *DS-GVO BDSG*, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 56a; Johannes/Geminn, *InTeR* 2021, S. 140, 143; Gärtner/Selzer, *DuD* 2023, S. 289, 291 f.; Weidenhammer/Gundlach, *DuD* 2018, S. 106, 106 f.; *DatKomm/Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 20; Bartels/Backer, *DuD* 2018, S. 214, 215.

Bewertung von TOM noch von Bedeutung sein. Dies bedarf aber erst an späterer Stelle einer genaueren Untersuchung.<sup>17</sup>

Für den Moment geht es um die Frage, ob sich die datenschutzrechtliche Bewertung von TOM unter das Kriterium „*Stand der Technik*“ subsumieren lässt. Für die Beantwortung dieser Frage reicht eine grundlegende Vorstellung über das Kriterium aus. Gerade im Kontext zu den anderen Begriffen „*Stand von Wissenschaft und Technik*“ und „*(allgemein anerkannte) Regeln der Technik*“ zeigt sich, dass es beim Stand der Technik erstmal ganz vereinfacht gesamt um die Machbarkeit geht, das geforderte Sicherheitsniveau umzusetzen.<sup>18</sup> Dies geht noch deutlicher aus dem Ratsentwurf der Datenschutz-Grundverordnung hervor, der auf „*verfügbare Technologien*“<sup>19</sup> abgestellt hat (vgl. Art. 30 Abs. 1 DS-GVO E (Rat)).<sup>20</sup> Ausgehend von der obigen Definition, dürfte im Rahmen des Kriteriums ferner noch die Zuverlässigkeit der Maßnahmen (hier die Sicherheit zu gewährleisten) zu beachten sein.

Sehr grob betrachtet, adressiert das Kriterium damit den (tatsächlichen) Aufwand der Datenverarbeiter, die Sicherheit zu gewährleisten. Gibt es bspw. keine Sicherheitsmaßnahmen, die ein entsprechendes Risiko adressieren oder (weiter) verringern können, dann kann dies einem höher anzusetzenden Sicherheitsniveau entgegenstehen. Das Kriterium kann daher als „Gegengewicht“ für den – anhand der Risikobewertung – plädierten Schutz fungieren.<sup>21</sup>

---

<sup>17</sup> Siehe Kap. 7, C., III. *Konkretisierung des ungeschriebenen Abwägungskriteriums der datenschutzrechtlichen Bewertung von TOM.*

<sup>18</sup> Vgl. Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 10; hierauf verweisend auch *DatKomm/Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 20; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 48, 56 f.; *Taeger/Gabel/Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 13, „*technisch möglich*“ und „*praktisch realisierbar*“; *Taeger/Pohle/Deusch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 316 (Stand: Mai 2022), fassen unter den Stand der Technik u.a. die „*Existenz einer bestimmten Technologie*“.

<sup>19</sup> Hervorhebung durch Verf.

<sup>20</sup> Rat der Europäischen Union, Ratsentwurf der DS-GVO, Ratsdokument 9565/15, vom 11.06.2015.

<sup>21</sup> *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 48, „*Gegenspieler*“; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 6, „*Korrektiv*“ und „*Grenze*“; vgl. auch *Ehmann/Selmayr/Hladjk*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 5, wonach das Schutzniveau gerade

Ausgehend von dieser sehr groben Definition lässt sich aber bereits sagen, dass sich die datenschutzrechtliche Bewertung von TOM nicht unter das Kriterium des Stands der Technik subsumieren lässt. Zwar stellt das Kriterium auf die Machbarkeit der Umsetzung ab. Dabei geht es aber wohl rein um die tatsächliche Verfügbarkeit und nicht ob irgendwelche Rechtsvorschriften der Implementierung von Maßnahmen entgegenstehen könnten. Eine Subsumtion der rechtlichen Bewertung von Sicherheitsmaßnahmen innerhalb des Kriteriums des Stands der Technik scheidet daher aus.<sup>22</sup>

## II. Implementierungskosten

Art. 32 Abs. 1 DS-GVO nennt als zweites Kriterium die „*Implementierungskosten*“<sup>23</sup>. Ähnlich wie der Stand der Technik bezieht sich auch dieses Kriterium auf die spätere Umsetzung der Sicherheit.<sup>24</sup> Anders als der Stand der Technik berücksichtigt das Kriterium dabei wirtschaftliche Faktoren bei der Umsetzung.<sup>25</sup>

---

unter Berücksichtigung des Stands der Technik und der Implementierungskosten abgewogen werden muss.

<sup>22</sup> A.A. wohl *Weidenbammer/Gundlach*, DuD 2018, S. 106, 109, die, allgemein und nicht unmittelbar zu Art. 32 DS-GVO, die Konformität mit Rechtsvorschriften als „*KO-Kriterium*“ bei der Bestimmung des Stands der Technik berücksichtigen wollen. Siehe auch *Bartels/Backer*, DuD 2018, S. 214, 217, die im Rahmen des Kriteriums Stand der Technik „*technische und rechtliche Faktoren*“ berücksichtigen möchten, zu den rechtlichen Faktoren allerdings nur auf Zertifikate i.S.d. Art. 32 Abs. 3 i.V.m. Art. 40 DS-GVO und die Bewertung des Risikos (hierzu sogleich) verweisen.

<sup>23</sup> Englisch: „*costs of implementation*“, Französisch: „*des coûts de mise en œuvre*“. Spanisch: „*los costes de aplicación*“, Italienisch: „*dei costi di attuazione*“, Niederländisch: „*de uitvoeringskosten*“.

<sup>24</sup> Vgl. *Simitis/Hornung/Spiecker gen. Döhmann/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 26; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 11; *Gola/Heckmann/Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 20; *DatKomm/Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 21; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 7; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 60 f.; *Johannes/Geminn*, InTeR 2021, S. 140, 144.

<sup>25</sup> *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 7; *Simitis/Hornung/Spiecker gen. Döhmann/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 26; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 60 f.; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 11; *Taeger/Gabel/Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-



Die Implementierung von TOM zur Gewährleistung des geforderten Schutzniveaus führt beim Datenverarbeiter zu entsprechenden Kosten. Durch das Kriterium „*Implementierungskosten*“ werden diese Kosten im Rahmen der Angemessenheit berücksichtigt. Das Ziel dieses Kriteriums liegt daher darin, dass die Kosten für die Gewährleistung der Sicherheit im Vergleich zum Risiko nicht außer Verhältnis stehen sollen.<sup>26</sup> Auch von seiner Funktion her ähnelt das Kriterium daher dem des Stands der Technik. Denn die „*Implementierungskosten*“ stehen eher auf der Gegenseite der Risikobewertung.<sup>27</sup>

Welche Kosten bei der Umsetzung der Sicherheit im Rahmen der Angemessenheitsprüfung berücksichtigt werden können, wie die Frage, ob auch Folgekosten umfasst sind,<sup>28</sup> ist für das Problem der Arbeit nur von nachrangiger Bedeutung und bedarf hier keiner abschließenden Klärung. Die grundlegende

---

GVO, Rn. 14; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 20 f.; *Johannes/Geminn*, InTeR 2021, S. 140, 144; *Gärtner/Selzer*, DuD 2023, S. 289, 291; siehe auch *DatKomm/Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 21, der neben dem finanziellen Aufwand auch den zeitlichen Aufwand hierunter berücksichtigen möchte, wobei zeitliche Faktoren sich wohl häufig auch finanziell bemerkbar machen (vgl. Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 21, aber ablehnend ggü. der unmittelbaren Berücksichtigung des zeitlichen Aufwands).

<sup>26</sup> *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 11; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 7; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 60 f.; *Taege/Gabel/Schultze-Melling*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 14; Gola/Heckmann/*Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 20.

<sup>27</sup> *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 48; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 6; siehe auch *Auernhammer/Kramer/Meints*, 8. Aufl. 2024, Art. 32 DS-GVO, Rn. 56 ff., die jedenfalls ausdrücklich nur in den Implementierungskosten ein „*Korrektiv*“ sehen und den Stand der Technik als „*Ausgangspunkt*“ betrachten (vgl. Rn. 53); vgl. *Johannes/Geminn*, InTeR 2021, S. 140, 144, wonach die Implementierungskosten „*zu den Sicherheitsanforderungen in Konkurrenz treten können*“ und die Rolle als „*Korrektiv*“ einnehmen; *Gärtner/Selzer*, DuD 2023, S. 289, 291, „*limitierende[r] Faktor*“.

<sup>28</sup> Siehe zu dem Problem der Folgekosten ausführlicher: Für eine Erfassung von Folgekosten *Simitis/Hornung/Spiecker* gen. *Döhm/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 26, *Gärtner/Selzer*, DuD 2023, S. 289, 291; *Bartels/Backer*, DuD 2018, S. 214, 217; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 11; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 8;

Funktion des Abwägungskriteriums liegt nämlich ausschließlich in der Berücksichtigung der wirtschaftlichen Auswirkungen bei der Gewährleistung der Sicherheit. Damit erlaubt auch dieses Kriterium keine Subsumtion der datenschutzrechtlichen Bewertung von TOM.

### III. Verarbeitungskriterium

Als Drittes nennt Art. 32 Abs. 1 DS-GVO das (hier zusammengefasste) Verarbeitungskriterium, bestehend aus „Art“<sup>29</sup>, „Umfang“<sup>30</sup>, „Umstände“<sup>31</sup> und „Zweck“<sup>32</sup> der Verarbeitung. Im Rahmen der Angemessenheitsprüfung berücksichtigt das Verarbeitungskriterium die zugrundeliegende Datenverarbeitung, also die Verarbeitung der Daten, die durch Art. 32 DS-GVO geschützt werden soll.<sup>33</sup>

---

Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 10, mit weiterführendem Verweis auf seine Kommentierung des Art. 25 DS-GVO, Rn. 45; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 60a mit einem Verweis auf seine Kommentierung des Art. 25 DS-GVO, Rn. 41, allerdings etwas kritisch hinsichtlich des Wortlauts; auch Schwartzmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 97 weist auf eine denkbar andere Wortlautinterpretation hin; ebenfalls kritisch aufgrund des Wortlauts und ohne eine finale Positionierung DatKomm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 22. Dagegen Johannes/Geminn, InTeR 2021, S. 140, 144; Schlegel, ZD 2020, S. 243, 246; wohl auch Kipker/Voskamp/Klein, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 25, die zwischen Implementierungs- und Folgekosten differenzieren und Folgekosten gerade keine Erwähnung fänden.

<sup>29</sup> Englisch: „the nature“, Französisch: „de la nature“, Spanisch: „la naturaleza“, Italienisch: „della natura“, Niederländisch: „de aard“.

<sup>30</sup> Englisch: „scope“, Französisch: „de la portée“, Spanisch: „el alcance“, Italienisch: „dell’oggetto“, Niederländisch: „de omvang“.

<sup>31</sup> Englisch: „context“, Französisch: „du contexte“, Spanisch: „el contexto“, Italienisch: „del contesto“, Niederländisch: „de context“.

<sup>32</sup> Englisch: „purposes“, Französisch: „des finalités“, Spanisch: „los fines“, Italienisch: „delle finalità“, Niederländisch: „de verwerkingsdoeleinden“, wobei die niederländische Sprachfassung für „die Zwecke der Verarbeitung“ einen zusammengesetzten Begriff aus „Zweck“ und „Verarbeitung“ – wie „Verarbeitungszweck“ – verwendet.

<sup>33</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 12; Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 24; Gierschmann u.a./Jergl, Datenschutz-Grundverordnung, 2018, Art. 32 DS-GVO, Rn. 20.

Anders als die beiden zuvor genannten Kriterien kommt dem Verarbeitungskriterium damit wohl eine andere Funktion im Rahmen der Angemessenheitsprüfung zu. Das Kriterium adressiert nicht den Aufwand bei der Umsetzung der Sicherheit, sondern steht in einem engen Zusammenhang mit der vorab durchzuführenden Risikobewertung.<sup>34</sup> Dies zeigt sich auch anhand von ErwG 76 DS-GVO, wonach das Risiko in Bezug auf die genannten Kriterien der Verarbeitung bestimmt wird.

Gerade weil das Verarbeitungskriterium sich nicht auf den Aufwand für die Umsetzung der Sicherheit bezieht, scheint eine Subsumtion der datenschutzrechtlichen Bewertung von TOM (die ebenfalls auf der Seite der Umsetzung steht) hierunter auf den ersten Blick nicht möglich. Fraglich ist jedoch, ob dem Kriterium eine „Doppelfunktion“ zukommen könnte. Jedenfalls im Rahmen der datenverarbeitenden TOM, die ihrerseits personenbezogene Daten verarbeiten, gäbe es schließlich eine (zweite) Datenverarbeitung, die dann im Rahmen des Verarbeitungskriteriums berücksichtigt werden könnte.

Die Annahme einer Doppelfunktion des Kriteriums ist aus zwei Gründen jedoch problematisch. Zunächst ließe sich eine solche Doppelfunktion dann wohl einzig auf datenverarbeitende TOM anwenden. Eine solche, spezifische Ausrichtung auf eine bestimmte Gruppe von TOM findet sich an keiner Stelle in Art. 32 DS-GVO. Weiterhin fehlt es aber auch generell an Anhaltspunkten, die überhaupt auf irgendeine Art einer Doppelfunktion dieses Abwägungskriteriums hinweisen könnten. Die Verordnung wollte mit dem Kriterium rein auf die – nach Art. 32 DS-GVO zu schützende – Verarbeitung abstellen und nicht allgemein auf involvierte Datenverarbeitungen, wie bspw. die Verarbeitung im Rahmen von datenverarbeitenden TOM. Wer dennoch eine Doppelfunktion annehmen möchte, trägt hierfür die Begründungslast<sup>35</sup>. Bis dahin scheidet eine

---

<sup>34</sup> Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 48, 55; Spindler/Schuster/Laue, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 5; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 12; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 85; Schlegel, ZD 2020, S. 243, 246; vgl. Johannes/Geminn, InTeR 2021, S. 140, 141, zur Bestimmung des Risikos anhand der Verarbeitungskriterien; siehe allgemein als Teil eines risikobasierten Ansatzes Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 22.

<sup>35</sup> Zur Begründungslast Krebs, AcP 195 (1995), S. 171 ff.

Subsumtion der datenschutzrechtlichen Bewertung von TOM unter das Verarbeitungskriterium aus.

#### IV. Risiko für die Rechte und Freiheiten betroffener Personen

##### 1. Allgemeines

Das letzte Kriterium des Art. 32 Abs. 1 Hs. 1 DS-GVO ist das „*Risiko für die Rechte und Freiheiten natürlicher Personen*“<sup>36</sup>. Wie zuvor bereits herausgearbeitet wurde, handelt es sich hierbei um den Ausgangspunkt der Prüfung des angemessenen Schutzniveaus.<sup>37</sup> Abweichend vom Wortlaut geht es daher strenggenommen um das „*Risiko für die Rechte und Freiheiten betroffener Personen*“.<sup>38</sup>

Mit der Aufnahme dieses Kriteriums in die Angemessenheitsprüfung dürfte die Verordnung damit lediglich klarmachen, dass dieses Risiko nicht alleine darüber entscheidet, welche Anforderungen an die Sicherheit der Verarbeitung zu stellen sind, sondern dass es vielmehr darauf ankommt, dieses Risiko mit den anderen Kriterien entsprechend abzuwägen.<sup>39</sup>

Inhaltlich befasst sich das Kriterium mit dem Risiko für die Rechte und Freiheiten betroffener Personen, das durch einen personal data breach während der Verarbeitung entstehen kann.<sup>40</sup> Die spätere Umsetzung der Sicherheit und damit die mögliche Berücksichtigung der datenschutzrechtlichen Bewertung von TOM sind daher vorrangig nicht von diesem Kriterium umfasst.

##### 2. Möglichkeit einer Doppelfunktion

Wie bereits beim Verarbeitungskriterium könnte auch hier an eine Doppelfunktion des Abwägungskriteriums überlegt werden. Denn eine Verarbeitung personenbezogener Daten im Rahmen datenverarbeitender TOM stellt gleichfalls

<sup>36</sup> Englisch: „*the risk [...] for the rights and freedoms of natural persons*“, Französisch: „*des risques [...] pour les droits et libertés des personnes physiques*“, Spanisch: „*riesgos [...] para los derechos y libertades de las personas físicas*“, Italienisch: „*del rischio [...] per i diritti e le libertà delle persone fisiche*“, Niederländisch: „*e risico's voor de rechten en vrijheden van personen*“.

<sup>37</sup> Siehe hierzu bereits Kap. 5, A. *Risikobewertung* (vgl. auch Kap. 4, B., II. *Risiko für die Rechte und Freiheiten (natürlicher) Personen*).

<sup>38</sup> Siehe zur Herleitung: Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>39</sup> Siehe hierzu bereits: Kap. 5, B., III., 1. *Problem des Bezugspunkts der Kriterien*.

<sup>40</sup> Siehe hierzu: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO*.

ein Risiko für die Rechte und Freiheiten (anderer) betroffener Personen dar und könnte daher von dem Kriterium ebenfalls umfasst sein.

Stellt man auf den eigentlichen Wortlaut ab, so dürfte zwar der Anwendungsbereich dieses Kriteriums mit dem Verweis auf das Risiko für die Rechte und Freiheiten *natürlicher* Personen weiter gefasst sein und wäre demnach nicht auf den sehr speziellen Fall der datenschutzrechtlichen Risiken im Rahmen datenverarbeitender TOM beschränkt. Dann müsste man allerdings erklären können, warum im Rahmen der Abwägung nun doch der weitere Begriff „natürliche Person“ statt „betroffene Person“ Anwendung finden sollte.

Für die Ziele des Art. 32 DS-GVO wurde diese Einschränkung des Begriffs – nach hier vertretener Ansicht – überzeugend hergeleitet.<sup>41</sup> Zwar kann ein Begriff innerhalb eines Rechtsakts im Rahmen einer funktionalen Auslegung auch unterschiedliche Bedeutungen haben.<sup>42</sup> Eine abweichende Auslegung nach der Funktion ist allerdings besonders zu begründen.<sup>43</sup> Eine solche Begründung lässt sich hier nicht finden. Denn zunächst wäre dies eine unterschiedliche Auslegung desselben Begriffs innerhalb derselben Vorschrift und vor allem desselben Absatzes, was ohne konkrete Hinweise wohl nicht anzunehmen ist. Ferner ist zu berücksichtigen, dass Art. 32 Abs. 1 DS-GVO nicht einfach nur denselben Begriff in Art. 32 Abs. 1 DS-GVO wörtlich verwendet. Art. 32 Abs. 1 DS-GVO greift für das angemessene Schutzniveau auf den Begriff und vor allem auch auf dieselbe Bedeutung innerhalb der Abwägung zurück, indem dort nur noch verkürzt von „dem Risiko“ gesprochen wird. Daher muss auch für den Begriff im Rahmen der Abwägungskriterien gelten, dass es sich hierbei um das Risiko für

---

<sup>41</sup> Siehe zur Herleitung: Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>42</sup> Siehe zur funktionalen Auslegung im Europäischen Recht statt vieler EuGH, verb. Rs. C-403/08, C-429/08 (Football Association Premier League u.a.), ECLI:EU:C:2011:631 = ZUM 2011, 803, Rn. 187 f.; Jung/Krebs/Stiegler/Krebs/Jung, *Gesellschaftsrecht in Europa*, 2019, § 2 Europäische Rechtsmethodik, Rn. 81. Siehe hierzu ausführlicher Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen* und dort die Nachweise in Fn. 142.

<sup>43</sup> Jung, *Spezifika der europäischen Methodenlehre*, in: *Das Vorabentscheidungsverfahren in der Zivilgerichtsbarkeit*, 2014, S. 17, 21, und Jung/Krebs/Stiegler/Krebs/Jung, *Gesellschaftsrecht in Europa*, 2019, § 2 Europäische Rechtsmethodik, Rn. 81, in beiden Werken wohl vorrangig bezogen auf eine Abweichung von einer Legaldefinition; siehe auch Riesenhuber/*Riesenhuber*, *Europäische Methodenlehre*, 4. Aufl. 2021, § 10, Rn. 20, allerdings vorrangig beim Vergleich zwischen verschiedenen Rechtsakten eines Rechtsgebiets; auch mit dem Fokus verschiedener Rechtsakte Beck, *The Legal Reasoning of the Court of Justice of the EU*, 2012, p. 192 f.

die Rechte und Freiheiten der – nach Art. 32 DS-GVO zu schützenden – betroffenen Person handelt.

Ähnlich wie oben, fehlt es damit an den entsprechenden Anhaltspunkten, die eine solche Doppelfunktion nahelegen könnten. Daher gilt auch hier, dass die Begründungslast<sup>44</sup> bei demjenigen liegt, der eine solche Doppelfunktion befürwortet. Bis dahin scheidet eine Subsumtion der datenschutzrechtlichen Bewertung unter dieses Kriterium aus.<sup>45</sup>

#### *V. Systematisierung und Zwischenergebnis*

Mit Blick auf den Inhalt der verschiedenen Abwägungskriterien scheint eine Subsumtion der datenschutzrechtlichen Bewertung von TOM unter die bestehenden Kriterien nicht möglich zu sein. Bei der näheren Betrachtung der einzelnen Abwägungskriterien zeigte sich jedoch eine Systematik, die für das allgemeine Verständnis an späterer Stelle noch von Bedeutung sein kann und daher hier dargestellt werden soll.

Ausgehend von ihrem Inhalt, lassen sich die vier Abwägungskriterien in Bezug auf ihre Funktion innerhalb der Angemessenheitsprüfung in zwei gegenüberstehende Gruppen einteilen. Die Kriterien „*Stand der Technik*“ und „*Implementierungskosten*“ beziehen sich auf die spätere Umsetzung der Sicherheit der Verarbeitung und berücksichtigen hierbei den Aufwand, der mit der Umsetzung der Sicherheit verbunden ist. Das Verarbeitungskriterium und das Risiko für die Rechte und Freiheiten betroffener Personen sagen hingegen etwas über die Schutzwürdigkeit der Verarbeitung bzw. der betroffenen Personen im Zusammenhang mit der Sicherheit der Verarbeitung aus. Die nachfolgende Grafik stellt dies einmal dar:

---

<sup>44</sup> Zur Begründungslast *Krebs*, AcP 195 (1995), S. 171 ff.

<sup>45</sup> Anders könnte man *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 43 verstehen, die bei einem Lösungsansatz über den Verhältnismäßigkeitsgrundsatz nach Art. 32 DS-GVO auf den „*Eingriff in die Rechte und Freiheiten der natürlichen Person*“ verweisen und damit die Terminologie dieses Kriteriums verwenden.

Aufwand zur Umsetzung der Sicherheit	Schutzwürdigkeit der Verarbeitung
- Stand der Technik	- Verarbeitungskriterium
- Implementierungskosten	- Risiko für die Rechte und Freiheiten betroffener Personen

Abb. 3: System der benannten Abwägungskriterien zur Bestimmung des angemessenen Schutzniveaus (eigene Darstellung)

Eine solche Systematik verwundert nicht, wenn man sich bewusst macht, dass es sich bei der Angemessenheitsprüfung eben um eine Verhältnismäßigkeitsprüfung handelt, bei der eine „Zweck-Mittel-Abwägung“<sup>46</sup> vorzunehmen ist.<sup>47</sup> Der Zweck i.d.S. liegt dann in dem Schutz der personenbezogenen Daten bei der Verarbeitung, während die Mittel den Aufwand durch die Implementierung technischer und organisatorischer Maßnahmen darstellen. Dennoch ist es für das allgemeine Verständnis von Vorteil, wenn man sich dieses Prinzip und die Umsetzung im Rahmen der Angemessenheitsprüfung konkret vor Augen führt.

<sup>46</sup> Siehe Koch, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, 2003, S. 37 f., der im „Zweck-Mittel-Ausgleich“ den „Kerngehalt“ des Verhältnismäßigkeitsbegriffs sieht und den „kleinsten gemeinsamen Nenner“ im Vergleich zwischen den Mitgliedstaaten. Vgl. Jarass, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 52 GrCh, Rn. 34, „Verhältnis zwischen [...] Belastung und [...] Ziel“ im Zusammenhang von Grundrechtseinschränkungen; Grabitz/Hilf/Nettesheim/Bast, Das Recht der Europäischen Union, Stand: 80. EL. 2023, Art. 5 EUV, Rn. 70 (Stand: August 2023), „Zweck-Mittel-Rationalität des Unionshandelns“, eher im Zusammenhang mit dem kompetenzbezogenen Verhältnismäßigkeitsgrundsatz, siehe aber auch Rn. 69a (Stand: August 2023); siehe auch Trstenjak/Beysen, EuR 2012, S. 265, 272, 280, die innerhalb einer „Angemessenheitskontrolle“ darauf abstellen, die „positiven Auswirkungen der überprüften Maßnahme“ hinsichtlich der Zielerreichung mit den „negativen Auswirkungen [...] auf andere [...] Rechtspositionen“ abzuwägen. Siehe auch von Danwitz, EWS 2003, S. 393, 398, jedoch kritisch zur Vorgehensweise des EuGH hinsichtlich einer „Angemessenheitsprüfung“ (399 f.).

<sup>47</sup> Siehe zum Gebot der Verhältnismäßigkeit im Rahmen der Angemessenheitsprüfung nach Art. 32 DS-GVO: Kap. 5, B., I. Bedeutung der Angemessenheit.

## C. Die datenschutzrechtliche Bewertung von TOM als ungeschriebenes Tatbestandsmerkmal der Abwägung

Die datenschutzrechtliche Bewertung von Sicherheitsmaßnahmen lässt sich nicht unter die bestehenden Abwägungskriterien subsumieren. Daher wäre zu überlegen, ob die datenschutzrechtliche Bewertung als ein ungeschriebenes Tatbestandsmerkmal (hier noch ohne eine methodische Einordnung zu verstehen) in die Abwägung aufgenommen werden kann.

### *I. Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO*

„Neue“ Abwägungskriterien können vom Rechtsanwender nicht willkürlich geschaffen werden, weil mit ihnen das Abwägungsergebnis beeinflusst wird und bedürfen in jedem Fall einer methodischen Rechtfertigung. Bevor methodisch gezeigt werden soll, wie sich gegebenenfalls ein entsprechendes Kriterium in die Angemessenheitsprüfung des Art. 32 DS-GVO integrieren lässt, sollte vorab zunächst untersucht werden, ob überhaupt der Bedarf für ein solches Kriterium besteht und ob es in die Systematik der Angemessenheitsprüfung passt.

#### *1. Die datenschutzrechtliche Bewertung als Aufrechterhaltung einer widerspruchsfreien Rechtsordnung*

Im bisherigen Verlauf der Arbeit wurde am Beispiel datenverarbeitender TOM bereits an mehreren Stellen der Bedarf für ein entsprechendes Kriterium aufgezeigt.<sup>1</sup> Einer ausführlichen Wiederholung der dort genannten Gründe bedarf es hier daher nicht mehr. Das wesentliche Argument für die Berücksichtigung der datenschutzrechtlichen Bewertung von Sicherheitsmaßnahmen im Rahmen der Angemessenheitsprüfung liegt in der Widerspruchsfreiheit der Rechtsordnung. Wie umfangreich im europäischen Recht von einer „Gesamtrechtsordnung“

---

<sup>1</sup> Siehe Kap. 2 Datenverarbeitende TOM im Regelungsbereich zwischen Art. 32 und Art. 6 DS-GVO und Kap. 6, C. Überarbeitung der Arbeitshypothese.



und demnach auch von einem Gebot ihrer Widerspruchsfreiheit auszugehen ist, ist noch nicht abschließend geklärt.<sup>2</sup>

Wie im 1. Teil gezeigt, droht im Rahmen datenverarbeitender TOM ein Widerspruch innerhalb der Datenschutz-Grundverordnung und damit innerhalb desselben Rechtsakts.<sup>3</sup> Auch wenn bezogen auf das gesamte Europäische Recht nicht von einer (widerspruchsfreien) Gesamtrechtsordnung ausgegangen werden kann, so muss jedoch mindestens innerhalb desselben Rechtsakt der Anspruch auf dessen Widerspruchsfreiheit bestehen.<sup>4</sup> Die Datenschutz-Grundverordnung kann nicht im Rahmen der Sicherheit der Verarbeitung zur Implementierung von Sicherheitsmaßnahmen verpflichtet (auch nicht mittelbar), wenn sie deren Implementierung an anderer Stelle (bspw. im Rahmen des Art. 6 DSGVO) verbietet.

Dieser Gedanke muss auch grundsätzlich gelten, obwohl Art. 32 DSGVO nicht zur Implementierung bestimmter Sicherheitsmaßnahmen verpflichtet. Alleine die Ausrichtung an ein Sicherheitsniveau, unter Berücksichtigung möglicherweise rechtswidriger Sicherheitsmaßnahmen, die im Anschluss nicht implementiert werden dürfen, rechtfertigt die Berücksichtigung der datenschutzrechtlichen Bewertung von Sicherheitsmaßnahmen im Rahmen der Angemessenheitsprüfung. Andernfalls käme es zu einer Verzerrung bei der Bestimmung des angemessenen Schutzniveaus.<sup>5</sup>

---

<sup>2</sup> Siehe hierzu ausführlicher Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 97; Riesenhuber/Riesenhuber, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 24 f.; Grundmann, RabelsZ 75 (2011), S. 882, 904 ff.; Martens, Methodenlehre des Unionsrechts, 2013, S. 411 ff. Jedenfalls damals gegen die Annahme einer auf Widerspruchsfreiheit gerichteten Gesamtrechtsordnung Höpfner/Rüthers, AcP 209 (2009), S. 1, 12. Siehe auch Rebbahn, ZfPW 2016, S. 281, 285 f., mit der Einordnung als eigene „Rechtsordnung“, die zwar „nicht alle Lebenssachverhalte und Rechtsfragen“ regelt, aber in den geregelten Bereichen „lückenlos“ sei.

<sup>3</sup> Siehe Kap. 2, A. Begründung eines Spannungsverhältnisses zwischen Art. 32 und Art. 6 DSGVO.

<sup>4</sup> In diese Richtung Martens, Methodenlehre des Unionsrechts, 2013, S. 415; vgl. Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 96, die allerdings darauf hinweisen, dass es Ausnahmefälle geben kann, in denen Widersprüche innerhalb eines Rechtsakts hinzunehmen sind.

<sup>5</sup> Siehe hierzu bereits: Kap. 6, C., III. Gefahr einer Verzerrung der Angemessenheit.

## 2. Die Berücksichtigung einzelner Sicherheitsmaßnahmen im jetzigen System der Abwägung

Ob allerdings ein Kriterium über die datenschutzrechtliche Bewertung von TOM auch in die bestehende Systematik der Angemessenheitsprüfung passt, ist damit noch nicht gesagt. Die gerade wieder angedeutete, notwendige Differenzierung zwischen der Sicherheit der Verarbeitung und einzelnen Sicherheitsmaßnahmen<sup>6</sup> könnte hier entgegenstehen.

Bei genauerer Betrachtung der bisherigen Abwägungskriterien zeigt sich aber, dass die Abwägung in einem begrenzten Umfang eine Anknüpfung an einzelne Sicherheitsmaßnahmen bereits jetzt vornimmt und hieraus Auswirkungen für die gesamte Sicherheit ableitet. Konkret geht es dabei um die Abwägungskriterien „Stand der Technik“ und „Implementierungskosten“. Die Angemessenheitsprüfung dient insgesamt dem Gebot der Verhältnismäßigkeit.<sup>7</sup> Der Stand der Technik und die Implementierungskosten berücksichtigen hierbei den Aufwand (i.w.S.) für die Implementierung der Sicherheit, der dann ins Verhältnis zu dem bestehenden Risiko zu setzen ist, um daraus einen angemessenen „Kompromiss“ an Sicherheit abzuleiten.<sup>8</sup> Der Stand der Technik berücksichtigt dabei sehr vereinfacht die tatsächliche Umsetzbarkeit,<sup>9</sup> während das Kriterium der Implementierungskosten die wirtschaftlichen Kosten umfasst.<sup>10</sup> Beide Kriterien müssen dabei aber im Zeitpunkt der Bestimmung des angemessenen Schutzniveaus zwangsläufig auf die zukünftige Umsetzung ausgerichtet sein. Sie beziehen sich daher auf die später (möglichen) Sicherheitsmaßnahmen.<sup>11</sup>

Damit ist bereits jetzt auf die Ebene der (einzelnen) Sicherheitsmaßnahmen abzustellen, wenn es um die Angemessenheit des Schutzniveaus geht. Zwar dürfte diese Berücksichtigung nicht dazu führen, dass ein hohes Sicherheitsniveau grds. an einzelnen Sicherheitsmaßnahmen scheitert. Denn man sollte nicht vergessen, dass diese Betrachtung der einzelnen Sicherheitsmaßnahmen dazu dient, ein angemessenes Schutzniveau insgesamt abzuleiten. An dieser Stelle kann es aber erstmal hintenanstehen, wie sich unterschiedliche Ausprägungen

---

<sup>6</sup> Ausführlicher: Kap. 7, A., I. *Zwingende Differenzierung zwischen Sicherheit und Sicherheitsmaßnahmen.*

<sup>7</sup> Siehe hierzu: Kap. 5, B., I. *Bedeutung der Angemessenheit.*

<sup>8</sup> Siehe hierzu: Kap. 7, B., V. *Systematisierung und Zwischenergebnis.*

<sup>9</sup> Siehe hierzu: Kap. 7, B., I. *Stand der Technik.*

<sup>10</sup> Siehe hierzu: Kap. 7, B., II. *Implementierungskosten.*

<sup>11</sup> Siehe jeweils: Kap. 7, B., I. *Stand der Technik* und Kap. 7, B., II. *Implementierungskosten.*

einzelner Abwägungskriterien auf das zu fordernde, angemessene Sicherheitsniveau auswirken.

Wichtig ist zunächst, dass bereits jetzt die Abwägungskriterien in einem begrenzten Umfang auf die Ebene der einzelnen Sicherheitsmaßnahmen abstellen. Ein weiteres Kriterium, wie das der datenschutzrechtlichen Bewertung dieser Sicherheitsmaßnahmen, das – neben tatsächlichen und wirtschaftlichen – auch rechtliche Aspekte berücksichtigt, wäre im System des Art. 32 DS-GVO jedenfalls kein Fremdkörper.

### 3. Die teleologische Rechtfertigung für ein eigenes Abwägungskriterium

Fraglich bleibt, ob die Berücksichtigung der datenschutzrechtlichen Bewertung der TOM nicht nur systematisch, sondern auch inhaltlich in die Angemessenheitsprüfung passen würde. Die grundlegende Rechtfertigung, einer widerspruchsfreien Rechtsordnung, für die Berücksichtigung eines solchen Kriteriums wurde ja schon dargelegt.<sup>12</sup> Zu klären bleibt aber noch, ob die datenschutzrechtliche Bewertung der TOM auch ein Teil der Angemessenheitsprüfung sein sollte.

Zu beachten ist dabei vor allem, dass es ohne die Berücksichtigung der datenschutzrechtlichen Bewertung nicht zwingend zu einem Widerspruch in der Rechtsordnung kommt. Nur dort, wo die Sicherheit der Verarbeitung nicht auf andere Weise umgesetzt werden kann, könnte ein solcher Widerspruch entstehen.<sup>13</sup> Zu einem erheblichen Teil hätte eine fehlende Berücksichtigung der datenschutzrechtlichen Bewertung Einfluss auf den Verhältnismäßigkeitsgedanken der Angemessenheitsprüfung.<sup>14</sup> Die Berücksichtigung der datenschutzrechtlichen Bewertung der TOM sollte daher vor allem auch in den Verhältnismäßigkeitsgedanken der Angemessenheitsprüfung passen.

Hierbei kann wieder ein Vergleich mit den bereits benannten Kriterien „Stand der Technik“ und „Implementierungskosten“ hilfreich sein. Beide Kriterien bringen das Interesse zum Ausdruck, dass die Umsetzung der Sicherheit der

---

<sup>12</sup> Siehe Kap. 7, C., I., 1. *Die datenschutzrechtliche Bewertung als Aufrechterhaltung einer widerspruchsfreien Rechtsordnung.*

<sup>13</sup> Siehe Kap. 6, C., I. „Pflicht“ zur Implementierung bestimmter (datenverarbeitender) TOM.

<sup>14</sup> Siehe Kap. 6, C., III. *Gefahr einer Verzerrung der Angemessenheit.*

Verarbeitung die Datenverarbeiter nicht über Gebühr belasten darf.<sup>15</sup> Das bestehende Risiko ist daher ins Verhältnis mit diesen Kriterien zu setzen, um daraus ein angemessenes und damit verhältnismäßiges Schutzniveau abzuleiten.

Beide Kriterien berücksichtigen damit den späteren tatsächlichen bzw. wirtschaftlichen „Aufwand“ bei der Umsetzung. Rechtliche Anforderungen an die Implementierung von technischen und organisatorischen Maßnahmen als eine Art „rechtlicher Aufwand“ werden in der Angemessenheitsprüfung jedoch nicht berücksichtigt. Die Ausführungen im Rahmen dieser Arbeit haben aber gezeigt, dass rechtliche Grenzen fast schon ähnliche Beschränkungen für die Umsetzung der Sicherheit der Verarbeitung bereithalten können, wie die tatsächliche Möglichkeit der Umsetzung.

Gerade im Vergleich zu dem Kriterium der „*Implementierungskosten*“ verwundert diese „Lücke“. Datenverarbeiter werden durch dieses Kriterium vor wirtschaftlich unverhältnismäßigen Nachteilen geschützt.<sup>16</sup> Anders als bei der technischen Machbarkeit geht es im Rahmen dieses wirtschaftlichen Kriteriums vor allem um die Verhältnismäßigkeit. Während man im Rahmen der tatsächlichen Umsetzung von Sicherheitsmaßnahmen auf das Problem stoßen kann, dass es keine Maßnahmen gibt, die einen höheren Schutz gewährleisten können, gibt es auf Seiten der „*Implementierungskosten*“ keine wirtschaftliche „Unmöglichkeit“ bei der Umsetzung der Sicherheit. Der wirtschaftliche Aufwand kann damit allenfalls unverhältnismäßig sein.<sup>17</sup>

In der Literatur wird dem Kriterium der „*Implementierungskosten*“ wohl eher eine untergeordnete Rolle zugesprochen. So wird herausgestellt, dass Datenverarbeiter einen „unzureichenden“ Schutz nicht aufgrund der wirtschaftlichen Belastung rechtfertigen können.<sup>18</sup> Diese Argumentation verkennt aber, dass die Entscheidung darüber, welches Schutzniveau gefordert wird und ob

---

<sup>15</sup> Siehe hierzu: Kap. 7, B., I. *Stand der Technik* und Kap. 7, B., II. *Implementierungskosten*.

<sup>16</sup> Statt vieler Spindler/Schuster/Laue, *Recht der elektronischen Medien*, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 7; siehe auch ausführlicher hierzu: Kap. 7, B., II. *Implementierungskosten*.

<sup>17</sup> Paal/Pauly/Martini, *DS-GVO BDSG*, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 60, „*wirtschaftlich Zumutbare*“; ähnlich Kühling/Buchner/Jandt, *DS-GVO – BDSG*, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 11; Taeger/Gabel/Schultze-Melling, *DSGVO – BDSG – TTDSG*, 4. Aufl. 2022, Art. 32 DS-GVO, Rn. 14, „*Wahrscheinlich zum Schutz vor unverhältnismäßigen wirtschaftlichen und finanziellen Belastungen*“.

<sup>18</sup> Plath/Grages, *DSGVO/BDSG/TTDSG*, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 4; BeckOK *Datenschutzrecht/Paulus*, Stand: 46. Ed. 2023, Art. 32 DS-GVO (Stand: November 2021), Rn. 9; *Johannes/Geminn*, *InTeR* 2021, S. 140, 145.

dies anschließend unzureichend erfüllt wurde, anhand der Abwägung der Angemessenheitskriterien zu erfolgen hat.<sup>19</sup> Teil dieser Angemessenheitsprüfung ist dabei auch die Berücksichtigung der Implementierungskosten. Wie stark das Kriterium im Rahmen der Abwägung zu berücksichtigen ist (also ab wann die Kosten unverhältnismäßig wären) und wie stark das Kriterium dann als „Gegengewicht“ wirkt, ist jedoch eine ganz andere Frage.

Andere begründen eine untergeordnete Rolle des Kriteriums dahingehend, dass die Implementierungskosten in Art. 24 DS-GVO, der als eine Art Generalvorschrift für (insb.) Art. 32 DS-GVO angesehen wird,<sup>20</sup> gerade keine Berücksichtigung finden.<sup>21</sup> Selbst wenn man Art. 24 DS-GVO hier als Generalvorschrift ansieht und in dessen Rahmen keine Implementierungskosten berücksichtigt werden dürfen, ändert dies aber nichts daran, dass die Sicherheit der Verarbeitung nach Art. 32 DS-GVO als speziellere Vorschrift ausdrücklich eine entsprechende Berücksichtigung vorsieht. Insofern würde der Grundsatz „*lex specialis derogat legi generali*“<sup>22</sup> greifen.

Daher kann man das Kriterium der Implementierungskosten nicht als nachrangig innerhalb des Art. 32 DS-GVO ansehen. Art. 32 Abs. 1 DS-GVO weist

---

<sup>19</sup> Siehe Kap. 5, B. *Angemessenheit des Schutzniveaus*.

<sup>20</sup> Kühling/Buchner/*Hartung*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 24 DS-GVO, Rn. 1; Taeger/Gabel/*Lang*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 24 DS-GVO, Rn. 2; Kipker/Reusch/Ritter/*Kipker*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 24 DS-GVO, Rn. 1 f.; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 7; Kipker/Reusch/Ritter/*Kipker*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 24 DS-GVO, Rn. 1 f.; vgl. Kipker/*Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 5 f.

<sup>21</sup> Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 26.

<sup>22</sup> Siehe zur generellen Anerkennung dieses Grundsatzes im Europäischen Recht: EuGH, Rs. C-128/11 (UsedSoft), ECLI:EU:C:2012:407 = ZUM 2012, S. 661, Rn. 56; EuGH, Rs. C-263/18 (Nederlands Uitgeversverbond und Groep Algemene Uitgevers), ECLI:EU:C:2019:1111 = GRUR 2020, S. 179, Rn. 55; EuGH, Rs. C-352/21 (A1 und A2 [Assurance d'un bateau de plaisance]), ECLI:EU:C:2023:344 = RdTW 2023, S. 345, Rn. 39; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 73 f.; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 428 f.; *Härtel*, Hdb. Europäische Rechtsetzung, 2006, § 15, Rn. 3.

den einzelnen Kriterien keine eigene Rangfolge zu.<sup>23</sup> Eine „Rangfolge“ ergibt sich allenfalls mittelbar aus der Funktion und Wirkungsweise der Abwägung selbst. Es ist daher auch hier noch einmal darauf hinzuweisen, dass man im Rahmen der konkreten Abwägung natürlich berücksichtigen muss, wie stark die einzelnen Kriterien zu bewerten sind. Das hat aber anhand der Verhältnismäßigkeitsprüfung und den konkreten Umständen zu erfolgen und ist nicht vorab gesetzlich durch eine Art Rangfolge definiert.

Der Einschätzung, dem Kriterium der „*Implementierungskosten*“ käme eine nachrangige Bedeutung zu, wird hier daher nicht vollumfänglich gefolgt. Denn der Schutz vor wirtschaftlicher Unverhältnismäßigkeit ist ebenfalls ein gerechtfertigtes Interesse, dass es im Rahmen der Abwägung umfassend zu berücksichtigen gilt. Eine detaillierte Auseinandersetzung in dieser Sache ist für die vorliegende Frage aber auch nicht entscheidend. Es geht auch nicht darum, dem – vom Gesetzgeber ausdrücklich verankerten – Kriterium seine Daseinsberechtigung abzuspreehen. Wichtig ist aber der Vergleich der Wertungen, die hinter dem Kriterium der „*Implementierungskosten*“ stehen und denen hinter dem „*Stand der Technik*“ und einem möglichen Kriterium über die datenschutzrechtliche Bewertung. Denn im Vergleich sind wirtschaftliche Aspekte „unbedeutender“ als rechtliche Vorgaben. Diesbezüglich kann man einfach sagen: Wenn die Angemessenheitsprüfung die wirtschaftlichen Interessen der Datenverarbeiter schützt, dann muss dies – im Rahmen eines Erst-recht-Schlusses –<sup>24</sup> auch für die Fälle gelten, in denen die Rechtsordnung den Datenverarbeitern Grenzen bei der Umsetzung der Sicherheit der Verarbeitung aufzeigt.

---

<sup>23</sup> Vgl. Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 26, „*keinen Vorrang einzelner Faktoren*“; wohl auch Bartels/Backer, DuD 2018, S. 214, 216, die wohl hinsichtlich dieser Kriterien keine „*Priorisierung*“ sehen.

<sup>24</sup> Siehe zum „Erst-recht-Schluss“ (oder „*argumentum a fortiori*“) als Argumentationstyp in der Europäischen Rechtsmethodik: EuGH, verb. Rs. C-200/07, C-201/07 (Marra), ECLI:EU:C:2007:356 = EuZW 2009, S. 23, Rn. 22; EuGH, Rs. C-210/06 (Cartesio), ECLI:EU:C:2008:723 = IStR 2009, S. 59, Rn. 76 f.; EuGH, Rs. C-17/10 (Toshiba Corporation e.a), ECLI:EU:C:2012:72 = EuZW 2012, S. 223, Rn. 86; Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 143; Beck, The Legal Reasoning of the Court of Justice of the EU, 2012, p. 220 f.; Martens, Methodenlehre des Unionsrechts, 2013, S. 327 f.

#### 4. Zwischenergebnis

Rechtspolitisch gibt es gute Gründe,<sup>25</sup> die datenschutzrechtliche Bewertung von Sicherheitsmaßnahmen im Rahmen der Angemessenheit des Schutzniveaus zu berücksichtigen. Neben dem grundlegenden Gedanken einer widerspruchsfreien Rechtsordnung zeigen sich innerhalb des Systems der Angemessenheitsprüfung Anhaltspunkte, die eine solche Berücksichtigung rechtfertigen. So kennt die bisherige Abwägung mit dem „Stand der Technik“ und den „Implementierungskosten“ bereits zwei Kriterien, die sich auf die spätere Umsetzung der Sicherheit beziehen und damit in ihrer Systematik mit einem Kriterium der datenschutzrechtlichen Bewertung von TOM vergleichbar wären.

Auch ein inhaltlicher Abgleich lässt darauf schließen, dass die Berücksichtigung rechtlicher Aspekte in die Angemessenheitsprüfung passt. Dies ergibt sich insbesondere aus einem Erst-recht-Schluss im Vergleich zum Kriterium der „Implementierungskosten“. Wenn die Angemessenheitsprüfung wirtschaftliche Beeinträchtigungen bei der Umsetzung der Sicherheit berücksichtigt, dann muss dies auch für rechtliche Hindernisse in diesem Zusammenhang gelten. Allgemein erscheint es so, dass die Angemessenheitsprüfung hierdurch sogar vervollständigt wird. Im Rahmen der Prüfung wären dann die tatsächlichen, wirtschaftlichen und rechtlichen Umstände bei der Umsetzung der Sicherheit der Verarbeitung zu berücksichtigen.

## II. Methodische Begründung

### 1. Darstellung möglicher Lösungswege

Ein entsprechendes Abwägungskriterium, wie die datenschutzrechtliche Bewertung von TOM bedarf nicht nur der inhaltlichen Legitimation, sondern muss auch methodisch gerechtfertigt werden. Hierfür stehen erstmal grundsätzlich mehrere Wege zur Verfügung.

---

<sup>25</sup> Siehe Kap. 7, C., I., 1. *Die datenschutzrechtliche Bewertung als Aufrechterhaltung einer widerspruchsfreien Rechtsordnung.*

Die Berücksichtigung der datenschutzrechtlichen Bewertung von TOM mittels einer direkten Subsumtion unter eines der genannten Abwägungskriterien (und damit als Teil dieses Kriteriums) scheidet nach der obigen Untersuchung aus.<sup>26</sup>

Der wohl regelungstechnisch unproblematischste und dazu rechtssicherste Weg wäre eine Lösung *de lege ferenda*. Im Rahmen einer Änderung der Datenschutz-Grundverordnung ließe sich ein entsprechendes Abwägungskriterium in Art. 32 DS-GVO ergänzen. Allerdings ist eine Änderung der Verordnung für die nächsten Jahre wohl nicht zu erwarten. Darauf deutet zumindest die erste Bewertung der Datenschutz-Grundverordnung durch die Europäische Kommission i.R.d. Verfahrens nach Art. 97 DS-GVO hin. Denn in ihrem Bericht sieht die Europäische Kommission zumindest nach aktueller Einschätzung noch keinen Bedarf für Änderungen an der Datenschutz-Grundverordnung.<sup>27</sup> Vielmehr möchte die Kommission die weiteren Entwicklungen abwarten und auf Basis weiterer Erfahrungen mit der Verordnung und der Rechtsprechung hierzu den Bedarf für zukünftige Änderungen prüfen.<sup>28</sup>

Zwar ist in diesem Zusammenhang anzumerken, dass die Europäische Kommission einen Verordnungsvorschlag<sup>29</sup> für Verfahrensregeln zur Durchsetzung der Datenschutz-Grundverordnung vorgelegt hat.<sup>30</sup> Dieser Vorschlag betrifft aber inhaltlich eben nur Verfahrensregeln und enthält somit gerade keine – wie hier untersuchten – materiell-rechtlichen Bestimmungen. Ferner zeigt das Vorhaben mittels einer gesonderten Verordnung, dass gerade keine Änderung an den bestehenden Regelungen geplant sein dürfte, die aber für das hier beschriebene Problem erforderlich wäre.

---

<sup>26</sup> Siehe hierzu: Kap. 7, B. *Subsumtion unter die Abwägungskriterien des Art. 32 Abs. 1 DS-GVO*.

<sup>27</sup> Europäische Kommission, Erster Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung, COM(2020) 264 final, vom 24.06.2020.

<sup>28</sup> Europäische Kommission, Erster Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung, COM(2020) 264 final, vom 24.06.2020, S. 19

<sup>29</sup> Europäische Kommission, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, COM(2023) 348 final, vom 04.07.2023.

<sup>30</sup> Siehe ausführlicher zu diesem Vorschlag: *Schild*, DuD 2023, S. 565 ff.; *Dehnert/Weber*, ZD 2023, S. 648 ff.



Ferner muss berücksichtigt werden, dass bereits die Verhandlungen zur Datenschutz-Grundverordnung langwierig und die Einigung nur unter einer Vielzahl von Kompromissen möglich war.<sup>31</sup> Für eine Änderung der Datenschutz-Grundverordnung müsste dieses einmal verabschiedete „Paket erneut aufgeschnürt“<sup>32</sup> werden. Der Versuch einer Änderung einzelner Regelungen der Datenschutz-Grundverordnung könnte demnach dazu führen, dass auch andere Teile oder sogar die gesamte Verordnung erneut zur Disposition gestellt werden und einen erneuten Kompromiss erschweren. Dieses Risiko könnte zumindest auch die Kommission gesehen haben, als sie ihren Vorschlag für Verfahrensregeln zur Durchsetzung der Datenschutz-Grundverordnung mittels einer eigenständigen Verordnung vorgelegt hat. Eine Lösung *de lege ferenda* kommt damit (realistisch) nicht in Betracht und könnte das Problem auch nur für die Zukunft lösen. Für aktuelle Fälle würde sie ohnehin nicht helfen.

Überlegenswert wäre auch die *de lege lata* Schaffung eines entsprechenden Abwägungstatbestands im Wege einer Rechtsfortbildung. Anders als das deutsche Recht unterscheidet die europäische Rechtsmethodik (begrifflich) nicht klar zwischen der Auslegung und der Rechtsfortbildung.<sup>33</sup> Dennoch kennt sie ent-

---

<sup>31</sup> Siehe für einen Überblick über das Gesetzgebungsverfahren: Simitis/Hornung/Spiecker gen. Döhmman/*Albrecht*, Datenschutzrecht, 2019, Einleitung, Rn. 184 ff.; Kühling/Buchner/*Kübling/Raab*, DS-GVO – BDSG, 4. Aufl. 2024, A. Einführung, Rn. 73 ff.; Taeger/Gabel/*Taeger/Schmidt*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Einführung zur DS-GVO, Rn. 22 ff. Siehe auch zum Gesetzgebungsverfahren und die Einigung zu wesentlichen Punkten unter Berücksichtigung der verschiedenen Entwürfe *Albrecht*, CR 2016, S. 88 ff.

<sup>32</sup> Siehe zur „*Paketlösung*“ als Verhandlungsinstrument und die damit zusammenhängenden Besonderheiten bei der Einigung *Jung/Krebs*, Die Vertragsverhandlung, 2016, S. 298, unter dem Stichpunkt: „*Paketlösung*“.

<sup>33</sup> *Walter*, Rechtsfortbildung durch den EuGH, 2009, S. 55 ff.; *Riesenhuber/Neuner*, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 2; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 10, 165; *Roth*, RabelsZ 75 (2011), S. 787, 820; *Rebhahn*, ZfPW 2016, S. 281, 286 f.; *Schön*, Die Analogie im Europäischen (Privat-)Recht, in: FS Canaris zum 80. Geburtstag, 2017, S. 147, 150; siehe auch *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 38 f., der eine solche Differenzierung (wohl auch inhaltlich) für das Europäische Recht für unangemessen hält. Kritisch zur fehlenden begrifflichen aber vor allem sachlichen Trennung *Höpfner/Rüthers*, AcP 209 (2009), S. 1, 5 f.; ebenfalls kritisch *Wank*, Juristische Methodenlehre, 2020, § 15, Rn. 5; auch *Schoch*, JZ 1995, S. 109, 116.

sprechende Instrumente, die nach deutschem Verständnis der Rechtsfortbildung zuzuordnen wären.<sup>34</sup> In Betracht käme hier die Schaffung eines unbenannten Abwägungstatbestands mittels einer teleologischen Reduktion.<sup>35</sup> Ein Rückgriff auf die Rechtsfortbildung, hier im Wege der teleologischen Reduktion, sollte aber erst erfolgen, wenn die Mittel der „einfachen“ Gesetzesauslegung nicht länger ausreichen, um einen „Missstand“ zu beheben.<sup>36</sup>

Zwar lässt sich die datenschutzrechtliche Bewertung von TOM nicht unter die (benannten) Abwägungskriterien subsumieren.<sup>37</sup> Darin erschöpft sich die Auslegung aber noch nicht. Denkbar wäre noch, dass die Verordnung die Abwägungskriterien zur Bestimmung der Angemessenheit nicht abschließend, sondern nur beispielhaft aufzählt. In diesem Fall könnte mittels der „einfachen“ Auslegung untersucht werden, ob es sich bei der datenschutzrechtlichen Bewertung von TOM um ein unbenanntes Abwägungskriterium einer nicht abschließenden Aufzählung handelt, das bereits von Beginn an Teil der Angemessenheitsprüfung ist.

---

<sup>34</sup> Riesenhuber/Neuner, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 7 ff.; Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 165 ff.; Walter, Rechtsfortbildung durch den EuGH, 2009, S. 134 ff., 161 ff.; Höpfner/Rüthers, AcP 209 (2009), S. 1, 17 ff. Siehe bereits die Verweise auf die „teleologische Reduktion“ und die „Analogie“ im europäischen Recht: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle* in den Fn. 106 und 107.

<sup>35</sup> Siehe allgemein zur – nach deutschem Verständnis – „teleologischen Reduktion“ im Europäischen Recht: Statt vieler EuGH, Rs. C-81/79 (Sorasio-Allo u.a./Kommission), ECLI:EU:C:1980:270 = BeckRS 2004, 73763, Rn. 15; Riesenhuber/Neuner, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 38 ff., siehe für weitere Nachweise: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle* und dort die Fn. 106.

<sup>36</sup> Siehe auch Höpfner/Rüthers, AcP 209 (2009), S. 1, 5 f., die u.a. auf die besondere Begründung hinweisen; wohl auch Schoch, JZ 1995, S. 109, 116, der die Unterscheidung zwischen „Auslegung“, „Rechtsfortbildung“ und „richterlicher Rechtsschöpfung“ im Lichte der „Funktionsordnung (-trennung)“ und „Organkompetenzen“ sieht; Rebbahn, ZfPW 2016, S. 281, 291, wonach die Rechtsfortbildung das Ergebnis der Auslegung voraussetzt, siehe auch kritisch zur Vorgehensweise des EuGH (S. 301). A.A. wohl Anweiler, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 38 f., der bereits die Unterscheidung zwischen Auslegung und Rechtsfortbildung ablehnt.

<sup>37</sup> Siehe hierzu: Kap. 7, B. *Subsumtion unter die Abwägungskriterien des Art. 32 Abs. 1 DSGVO*.

## 2. Abschließende oder offene Aufzählung der Abwägungskriterien

### a) Grundlage

In der Literatur wird der abschließende bzw. nicht abschließende Charakter der Abwägungskriterien kaum diskutiert. Aufgrund fehlender Formulierungen, die auf eine offene Aufzählung schließen lassen („insbesondere“, „unter anderem“, „wie“, etc.), liegt der Schluss nahe, dass die Abwägungskriterien in Art. 32 Abs. 1 DS-GVO abschließend aufgezählt werden. Dort wo auf eine nicht abschließende Aufzählung verwiesen wird, fehlt es jedoch an einer Begründung.<sup>38</sup>

Auch wenn es an entsprechenden Hinweisen auf eine nicht abschließende Auflistung mangelt, ergeben sich dennoch Zweifel, ob Art. 32 DS-GVO die Kriterien zur Bestimmung des angemessenen Schutzniveaus wirklich abschließend aufzählt. Den Ausgangspunkt bilden zunächst teleologische Überlegungen. Wie bereits festgestellt, adressiert die Abwägung das Gebot der Verhältnismäßigkeit und will einen Ausgleich zwischen dem Schutz vor dem Risiko für die Rechte und Freiheiten betroffener Personen und dem erforderlichen Aufwand zur Vermeidung oder Senkung dieses Risikos schaffen. Wie oben bereits erarbeitet, entstünde innerhalb dieser Verhältnismäßigkeitsprüfung jedenfalls eine „Lücke“, wenn man rechtliche Faktoren bei der Umsetzung der Sicherheit nicht berücksichtigen würde.<sup>39</sup>

Auch innerhalb der Vorschrift des Art. 32 DS-GVO selbst erwachsen Zweifel an einer abschließenden Aufzählung. Denn bei genauerer Betrachtung des Art. 32 DS-GVO lassen sich entsprechende Hinweise auf einen nicht abschließenden Charakter der Abwägungskriterien ausmachen. Dass diese Hinweise nicht gleich erkannt werden, dürfte wieder der etwas missverständlichen Regelungstechnik des Art. 32 DS-GVO geschuldet sein. Wie zu Beginn des 2. Teils anhand mehrerer Beispiele darauf hingewiesen wurde, ist Art. 32 DS-GVO sowohl in vielen Formulierungen als auch in seiner Systematik missverständlich formuliert.<sup>40</sup> Hinweise für eine nicht abschließende Aufzählung könnten sich aus Art. 32 Abs. 2 DS-GVO ergeben.

---

<sup>38</sup> Kuner/Bygrave/Docksey/Burton, GDPR, 2020, p. 636.

<sup>39</sup> Siehe hierzu: Kap. 7, C., I. *Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO.*

<sup>40</sup> Siehe hierzu: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO.*

Bereits zuvor wurde darauf hingewiesen, dass Art. 32 Abs. 2 DS-GVO an das angemessene Schutzniveau nach Art. 32 Abs. 1 DS-GVO anknüpft und hierbei wohl konkretisieren möchte, wie dieses zu bestimmen ist.<sup>41</sup> Weiterhin wurde erarbeitet, dass sich Art. 32 Abs. 2 DS-GVO – jedenfalls ausgehend des Wortlauts – wohl nicht nur einer, sondern gleich zwei nicht abschließender Aufzählungen bedient.<sup>42</sup> Ausgehend von dem Anknüpfungspunkt des angemessenen Schutzniveaus in Art. 32 Abs. 2 DS-GVO dürfte sich eine dieser Aufzählungen auf die Angemessenheitsprüfung insgesamt beziehen. Sie könnte damit als Mittel dienen, die datenschutzrechtliche Bewertung von TOM als Kriterium bei der Angemessenheitsprüfung zu berücksichtigen. Wie bereits dargelegt, sind die beiden Aufzählungen auf verschiedenen Ebenen angesiedelt.<sup>43</sup> Welche Funktionen den jeweiligen Aufzählungen im System des Art. 32 DS-GVO zukommt, soll nachfolgend untersucht und anhand der Problemstellung bewertet werden.

#### *b) Offene Aufzählung der (inneren) zweiten Ebene*

Den Anfang soll die zweite Aufzählung des Art. 32 Abs. 2 DS-GVO machen. Im Rahmen dieser zweiten Aufzählung konkretisiert die Verordnung den Begriff der „Risiken, die mit der Verarbeitung verbunden sind“, indem sie diese „Risiken“ beispielhaft aufzählt.<sup>44</sup> Systematisch betrachtet ist die zweite Aufzählung ein Teil der ersten Aufzählung, die u.a. die „Risiken, die mit der Verarbeitung verbunden sind“ umfasst.<sup>45</sup> Man kann insofern auch von einer Aufzählung auf zweiter oder innerer Ebene sprechen.

Der Inhalt und die Funktion dieser zweiten Aufzählung des Art. 32 Abs. 2 DS-GVO wurde bereits ausgiebig zu Beginn des 2. Teils thematisiert.<sup>46</sup>

---

<sup>41</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO* und Kap. 5, B., II. *Bestimmung der Angemessenheit nach Art. 32 Abs. 2 DS-GVO*.

<sup>42</sup> Siehe hierzu: Kap. 5, B., II., 1. *Die offenen Aufzählungen des Art. 32 Abs. 2 DS-GVO*.

<sup>43</sup> Siehe hierzu: Kap. 5, B., II. *Bestimmung der Angemessenheit nach Art. 32 Abs. 2 DS-GVO* und insbesondere dort unter 3. *Systematisierung des Art. 32 Abs. 2 DS-GVO* die Abb. 2: *Ebenen der Aufzählungen des Art. 32 Abs. 2 DS-GVO (eigene Darstellung)*.

<sup>44</sup> Siehe hierzu und zur Kritik an dieser beispielhaften Aufzählung: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle*.

<sup>45</sup> Siehe hierzu auch die Abb. 2: *Ebenen der Aufzählungen des Art. 32 Abs. 2 DS-GVO (eigene Darstellung)* unter: Kap. 5, B., II., 3. *Systematisierung des Art. 32 Abs. 2 DS-GVO*.

<sup>46</sup> Siehe hierzu: Kap. 4, C. *Personal data breaches (und andere Sicherheitsvorfälle)*.

Unter dem irreführenden Begriff der „Risiken, die mit der Verarbeitung verbunden sind“ definiert Art. 32 Abs. 2 DS-GVO die Gefahren, die die Sicherheit der Verarbeitung adressieren möchte.<sup>47</sup> Mit Ausnahme der wohl nicht abschließenden Auflistung dieser Gefahren, entsprechen diese dem Begriff des personal data breach nach Art. 4 Nr. 12 DS-GVO.<sup>48</sup> Diese Abweichung wurde mit Blick auf die zugrundeliegende Systematik der Vorschriften der Art. 32, 33, 34 DS-GVO und der Definition nach Art. 4 Nr. 12 DS-GVO zwar kritisiert und sollte im Wege einer teleologischen Reduktion des Art. 32 Abs. 2 DS-GVO auf den Anwendungsbereich des personal data breach begrenzt werden.<sup>49</sup> Mit Blick auf den vorliegenden Untersuchungsgegenstand bedurfte dies jedoch keiner abschließenden Klärung.

Ob sich hinsichtlich der Suche nach einer Anknüpfung eines Kriteriums über die datenschutzrechtliche Bewertung von TOM an die Angemessenheitsprüfung hieran etwas ändert, ist zu bezweifeln. Die Funktion des Tatbestands der „Risiken, die mit der Verarbeitung verbunden sind“, bleibt auch unter Berücksichtigung dieses Problem weiterhin klar. Es handelt sich um die zu adressierten Gefahren, aus denen sich ein Risiko für die Rechte und Freiheiten betroffener Personen ergeben kann. Als immanenter Bestandteil des Risikos für die Rechte und Freiheiten betroffener Personen gehen sie zwar gemeinsam mit diesem in die Angemessenheitsprüfung ein. Eine „Ergänzung“ dieser – hier abzulehnenden – nicht abschließenden Aufzählung von Gefahren durch die datenschutzrechtliche Bewertung von TOM passt jedoch weder in die Systematik der Abwägung als solche noch in das Kriterium des Risikos für die Rechte und Freiheiten betroffener Personen.<sup>50</sup>

Die nicht abschließende Aufzählung der (inneren) zweiten Ebene des Art. 32 Abs. 2 DS-GVO kann somit nicht als methodische Rechtfertigung dienen.

---

<sup>47</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO.*

<sup>48</sup> Siehe hierzu: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle.*

<sup>49</sup> Siehe hierzu: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle.*

<sup>50</sup> Siehe hierzu bereits die Frage nach einer Doppelfunktion des Abwägungskriteriums: Kap. 7, B., IV., 2. *Möglichkeit einer Doppelfunktion.*

c) Offene Aufzählung der (äußeren) ersten Ebene

aa) Grundlagen

Die erste Aufzählung in Art. 32 Abs. 2 DS-GVO liegt auf einer übergeordneten Ebene, denn die „Risiken, die mit der Verarbeitung verbunden sind“ sind ein Teil dieser Aufzählung. Diese „Risiken“ sind jedoch das einzige Kriterium, das die Verordnung im Rahmen dieser Aufzählung benennt. Mit der einleitenden Formulierung „insbesondere“<sup>51</sup> macht die Verordnung doch auch hier klar, dass es sich hierbei nicht um das einzige Kriterium handeln soll. Welche weiteren Kriterien unter diese Aufzählung fallen, bleibt allerdings unklar. Dies wurde bereits an anderer Stelle kritisiert, da eine nicht abschließende Aufzählung zu einem erheblichen Teil anhand der benannten Kriterien zu konkretisieren ist und Art. 32 Abs. 2 DS-GVO damit nur wenig Hilfe bei der Auslegung bietet.<sup>52</sup>

Bei der Frage, ob die Kriterien der Angemessenheitsprüfung nach Art. 32 Abs. 1 DS-GVO abschließend oder offen formuliert sind, erlangen die nicht benannten Punkte der ersten Aufzählung des Art. 32 Abs. 2 DS-GVO allerdings an Bedeutung. So könnte man sich die Frage stellen, ob die (vermeintlich) abschließende Aufzählung der Angemessenheitskriterien in Art. 32 Abs. 1 Hs. 1 DS-GVO nicht ein Teil der offenen, ersten Aufzählung des Art. 32 Abs. 2 DS-GVO sein könnte.

bb) Die erste Aufzählung des Art. 32 Abs. 2 DS-GVO als echte, offene Aufzählung

Bei dieser Frage ist vorab zu klären, ob es sich im Rahmen des Art. 32 Abs. 2 DS-GVO tatsächlich um eine offene Aufzählung handelt. Der Wortlaut von Art. 32 Abs. 2 DS-GVO ist mit der Formulierung „insbesondere“<sup>53</sup> eindeutig. Dennoch kann das vermeintlich eindeutige Wortlautargument hier nicht ausreichen. Vor dem Hintergrund, dass gerade der Wortlaut und die Systematik des Art. 32 DS-GVO innerhalb dieser Arbeit deutlich kritisiert wurden,<sup>54</sup> bedarf es im Wege der Auslegung weiterer Hinweise, die auf eine offene Aufzählung schließen.

<sup>51</sup> Englisch: „in particular“, Französisch: „en particulier“, Spanisch: „particularmente“, Italienisch: „in special modo“, Niederländisch: „met name“.

<sup>52</sup> Hierzu bereits: Kap. 5, B., II., 3. Systematisierung des Art. 32 Abs. 2 DS-GVO.

<sup>53</sup> Englisch: „in particular“, Französisch: „en particulier“, Spanisch: „particularmente“, Italienisch: „in special modo“, Niederländisch: „met name“.

<sup>54</sup> Siehe hierzu insbesondere nur: Kap. 4 Das allgemeine Regelungsziel des Art. 32 DS-GVO.

Ein Argument, dass gegen eine offene Aufzählung und daher für einen fehlerhaften Wortlaut spricht, könnte im Vergleich zur Vorgängerregelung des Art. 17 DS-RL gesehen werden. Denn eine, mit Art. 32 Abs. 2 DS-GVO vergleichbare Regelung fand sich in Art. 17 DS-RL nicht. Gleichzeitig bestand wohl auf Seiten des Gesetzgebers das Interesse, Art. 32 DS-GVO nach dem Vorbild von Art. 17 DS-RL zu schaffen.<sup>55</sup> Ob der Gesetzgeber mit Art. 32 Abs. 2 DS-GVO bewusst von dem Vorbild aus der Datenschutzrichtlinie abweichen wollte, ist soweit nicht ersichtlich. Die Abweichung von Art. 17 DS-RL könnte daher auch ein Redaktionsversehen innerhalb des Art. 32 DS-GVO sein und zu dem Ergebnis führen, dass Art. 32 Abs. 2 DS-GVO im Zusammenhang mit der Bestimmung des angemessenen Schutzniveaus keine offene Aufzählung in einem vergleichbaren Sinne vorsieht. Art. 32 Abs. 2 DS-GVO hätte damit nur die Funktion, das Risiko für die Rechte und Freiheiten betroffener Personen dahingehend zu konkretisieren, dass es sich hierbei um einen Sicherheitsvorfall handelt, wie dies noch in Art. 17 Abs. 1 DS-RL deutlicher zum Ausdruck kam.<sup>56</sup>

Im Rahmen einer solchen, historischen Auslegung darf auf die Datenschutzrichtlinie aber nur mit Vorsicht verwiesen werden. Nur weil die Datenschutz-Grundverordnung sich Art. 17 DS-RL zum Vorbild genommen hat, bedeutet das nicht, dass Abweichungen gleich einen Fehler bedeuten müssen. Dies gilt einmal allgemein, da es gerade das Ziel der Datenschutz-Grundverordnung war, den Datenschutz zu modernisieren (vgl. ErwG 6 f. DS-GVO).<sup>57</sup> Änderungen sind dabei zwangsweise notwendig. Zum anderen gilt dies auch speziell für Art. 32 DS-GVO. Denn hätte es der Gesetzgeber gewollt, dass Art. 17 DS-RL vollständig in der Datenschutz-Grundverordnung wieder auflebt, dann hätte er wohl den Wortlaut aus der Richtlinie – wenigstens in den relevanten Teilen – vollständig übernommen. Dass dies aber gerade nicht geschehen ist, zeigte sich

---

<sup>55</sup> Siehe statt vieler Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 2 f., a.A. wohl Sander, PinG 2017, S. 250, 252 f. Siehe auch: Kap. 5, B., III., 3. *Historische Auslegung* und dort insb. Fn. 55.

<sup>56</sup> Siehe hierzu: Kap. 5, B., III., 3. *Historische Auslegung*.

<sup>57</sup> Vgl. Europäische Kommission, Kommissionsentwurf der DS-GVO, KOM(2012) 11 endgültig, vom 25.01.2012, S. 1 f. Siehe kritisch zur Erfüllung dieses Ziels Roßnagel, DuD 2016, S. 561 ff.; Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 1, Rn. 27 ff., insb. 41 f. hinsichtlich des Ziels der Modernisierung; Kühling/Martini, EuZW 2016, S. 448 ff., die in der Datenschutz-Grundverordnung eher eine „*Evolution*“ als einer „*Revolution*“ des europäischen Datenschutzrechts sehen.

bereits zuvor bei einem Vergleich der beiden Vorschriften.<sup>58</sup> In Art. 32 DS-GVO leben zwar wesentliche Kerngedanken aus Art. 17 DS-RL auf. Im Detail hat die Vorschrift aber dennoch eine deutliche Änderung erfahren, die nicht darauf schließen lässt, dass der Gesetzgeber Art. 17 DS-RL vollständig übernehmen wollte. Art. 32 Abs. 2 DS-GVO könnte daher das Ergebnis eines solchen Änderungswunsches gewesen sein. Die Auslegung anhand der historischen Entwicklung der Vorschrift liefert daher nur wenige Anhaltspunkte.

Entscheidende Anhaltspunkte für die Auslegung dürfte sich daher wohl vorrangig aus dem Telos der Angemessenheitsprüfung ergeben. Fest steht, dass Art. 32 Abs. 2 DS-GVO die Bestimmung des angemessenen Schutzniveaus nach Art. 32 Abs. 1 DS-GVO konkretisieren möchte.<sup>59</sup> Dabei stellt Art. 32 Abs. 2 DS-GVO auch allgemein auf das *angemessene* Schutzniveau ab und will sich damit wohl nicht auf einzelne Teile davon konzentrieren. Dies spricht erstmal dafür, dass es neben dem genannten Kriterium der „Risiken, die mit der Verarbeitung verbunden sind“ noch weitere Kriterien geben dürfte und die Aufzählung nach Art. 32 Abs. 2 DS-GVO damit nicht abschließend formuliert ist. Denn die „Risiken, die mit der Verarbeitung verbunden sind“ definieren die Gefahren auf deren Basis das Risiko für die Rechte und Freiheiten betroffener Personen zu ermitteln ist und stellen eine Konkretisierung dieses Risikos dar.<sup>60</sup> Sie liegen dem angemessenen Schutzniveau daher als Teil des Risikos bereits zugrunde.<sup>61</sup> Damit sind sie aber auch nur auf einen kleinen Ausschnitt bei der Bestimmung des angemessenen Schutzniveaus beschränkt. Eine umfassende Abwägung aller Umstände bei der Bestimmung des angemessenen Schutzniveaus dürfte dann auch dem zugrundeliegenden Gebot der Verhältnismäßigkeit gerecht werden.

Isoliert betrachtet ist es schwer zu sagen, ob die Formulierung „*insbesondere*“ und damit der Hinweis auf eine offene Aufzählung vom Gesetzgeber beabsichtigt war oder versehentlich aufgenommen wurde. Der klare Wortlaut lässt auf eine offene Aufzählung schließen. Weiterhin zeigen sich erstmal keine eindeutigen Hinweise in anderen Auslegungsmethoden, die für einen Fehler sprechen. Daher ist zunächst davon auszugehen,<sup>62</sup> dass der Gesetzgeber die Formulierung

<sup>58</sup> Siehe hierzu: Kap. 5, B., III., 3. *Historische Auslegung*.

<sup>59</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO*.

<sup>60</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO*.

<sup>61</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO*.

<sup>62</sup> Siehe zur Begründungslast Krebs, AcP 195 (1995), S. 171 ff.



so beabsichtigt hatte und demnach auch eine nicht abschließende Aufzählung hier in Art. 32 Abs. 2 DS-GVO zugrunde legen wollte.

*cc) Systematische Widersprüche?*

Weiterhin steht die berechnete Frage im Raum, wieso man eine Aufzählung von Kriterien aus einem Absatz (Art. 32 Abs. 1 DS-GVO) in eine nicht abschließende Aufzählung eines anderen Absatzes (Art. 32 Abs. 2 DS-GVO) integrieren sollte. Beide Aufzählungen hat der Gesetzgeber doch scheinbar klar durch unterschiedliche Absätze voneinander getrennt. Hätte der Gesetzgeber gewollt, dass die Abwägungskriterien nach Art. 32 Abs. 1 DS-GVO im Lichte der ersten Aufzählung nach Art. 32 Abs. 2 DS-GVO betrachtet werden, dann hätte er sie ohne weiteres direkt in Art. 32 Abs. 2 DS-GVO aufnehmen können.

Grundsätzlich handelt es sich hierbei um ein gewichtiges, systematisches Argument, das aufgrund der besonderen Umstände aber hier zurückhaltend zu berücksichtigen ist. Wie bereits mehrfach dargelegt, zeigen sich u.a. in Bezug auf die Systematik deutliche Konstruktionsschwächen in Art. 32 DS-GVO.<sup>63</sup> Zwar folgt die Vorschrift einer klaren Gesetzssystematik. Diese wird im Normtext aber nicht klar ausgedrückt, sondern lässt sich zu einem großen Teil eher aus dem Telos der Vorschrift und dem (erkennbaren) Regelungsbereich ableiten. Die Aufspaltung in zwei Absätze kann daher auch auf eine „unsaubere“ Regelungstechnik zurückzuführen sein.

Hinweise die auf eine Verbindung beider Aufzählungen deuten, zeigen sich wiederum dadurch, dass Art. 32 Abs. 2 DS-GVO klar die Bestimmung des angemessenen Schutzniveaus nach Art. 32 Abs. 1 DS-GVO konkretisieren möchte. Mit den „Risiken, die mit der Verarbeitung verbunden sind“, konkretisiert Art. 32 Abs. 2 DS-GVO die Gefahren für die Rechte und Freiheiten betroffener Personen nach Art. 32 Abs. 1 DS-GVO.<sup>64</sup> Diese Konkretisierung wirkt sich aber überwiegend auf den ersten Schritt der Prüfung des angemessenen Schutzniveaus aus, indem es die Risikobewertung beeinflusst. Im Rahmen der anschließenden Angemessenheitsprüfung ist das Risiko für die Rechte und Freiheiten betroffener Personen (und damit die Gefahren nach Art. 32 Abs. 2 DS-

---

<sup>63</sup> Siehe hierzu: Kap. 4 *Das allgemeine Regelungsziel des Art. 32 DS-GVO.*

<sup>64</sup> Siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO.*

GVO) zwar dann ebenfalls zu berücksichtigen.<sup>65</sup> Für die *Angemessenheit* dürfen dann aber vor allem die, dem Schutz „entgegenstehenden“, Kriterien von Bedeutung sein. Diese finden einzig durch die Berücksichtigung der Gefahren nach Art. 32 Abs. 2 DS-GVO allerdings noch keine Beachtung, obwohl Art. 32 Abs. 2 DS-GVO hier klar auf das *angemessene* Schutzniveau verweist.

*dd) Doch unterschiedliche Bezugspunkte der Kriterien?*

Die Argumentation über Art. 32 Abs. 2 DS-GVO als (weitreichende) Konkretisierung des angemessenen Schutzniveaus nach Art. 32 Abs. 1 DS-GVO wirft jedoch wieder eine grundlegende Frage auf, die eigentlich im Zusammenhang mit den Anforderungen an die Sicherheit der Verarbeitung geklärt zu sein schien. Aufgrund der wohl bestehenden systematischen „Widersprüche“ ist erneut die Frage zu stellen, ob sich die Abwägungskriterien nach Art. 32 Abs. 1 DS-GVO nicht doch auf die Auswahl der technischen und organisatorischen Maßnahmen beziehen und mit der Bestimmung des angemessenen Schutzniveaus als solches nichts zu tun haben.<sup>66</sup> Dieses würde dann ausschließlich von Art. 32 Abs. 2 DS-GVO bestimmt.

Doch selbst unter Berücksichtigung eines drohenden, systematischen „Widerspruchs“ bzw. eher eines Mangels in der Normstruktur, überzeugen die Argumente und die Einordnung oben weiterhin.<sup>67</sup> Es würde schlicht keinen Sinn ergeben, Anforderungen an die Auswahl technischer und organisatorischer Maßnahmen zu stellen, wenn diese nicht gleichzeitig auf die Ebene des angemessenen Schutzniveaus einwirken. Aufgrund seiner Zielorientiertheit ist nach Art. 32 DS-GVO ausschlaggebend, ein angemessenes Schutzniveau zu gewährleisten. Wie dieses Schutzniveau zu gewährleisten ist, ist (für Art. 32 DS-GVO) dabei nicht relevant und sollte auch nach den allgemeinen Schutzziele des Art. 32 DS-GVO keine Relevanz haben.<sup>68</sup>

Einen möglichen weiteren, noch nicht geprüften (dritten) Bezugspunkt für die Abwägungskriterien nach Art. 32 Abs. 1 DS-GVO gibt es in der Vorschrift

---

<sup>65</sup> Siehe hierzu: Kap. 5, B., I. *Bedeutung der Angemessenheit* und Kap. 7, B., IV., 1. *Allgemeines*.

<sup>66</sup> Siehe hierzu: Kap. 5, B., III., 1. *Problem des Bezugspunkts der Kriterien*.

<sup>67</sup> Siehe hierzu: Kap. 5, B., III., 5. *Eigene Lösung*.

<sup>68</sup> Siehe hierzu: Kap. 5, C., V., 3. *Zielorientierte Pflicht*.

ebenfalls nicht. Unter Inkaufnahme systematischer Mängel können sich die Kriterien nach Art. 32 Abs. 1 DS-GVO daher (auch) nur auf das angemessene Schutzniveau beziehen.

*ee) Eigene Lösung*

Festgestellt werden kann, dass Art. 32 Abs. 2 DS-GVO bei der Bestimmung des angemessenen Schutzniveaus zu berücksichtigen ist. Aufgrund der erfolgten Untersuchung ist es im Ergebnis auch überzeugend anzunehmen, dass Art. 32 Abs. 2 DS-GVO die Kriterien, die dabei zu berücksichtigen sind, nicht abschließend aufzählt. Gleichzeitig sind aber auch die Kriterien nach Art. 32 Abs. 1 DS-GVO bei der Angemessenheit des Schutzniveaus zu berücksichtigen und miteinander abzuwägen. Dieses Nebeneinander der verschiedenen Faktoren, die über zwei Absätze verteilt sind, mag aus regelungstechnischer und systematischer Sicht missglückt sein, lässt sich aber aufgrund des Normzwecks anders nur schwer erklären. Um dennoch eine Systematik innerhalb des Art. 32 DS-GVO zu schaffen, sollte man daher die Kriterien des Art. 32 Abs. 1 DS-GVO als Teil der nicht abschließenden Aufzählung des Art. 32 Abs. 2 DS-GVO betrachten.

*d) Zwischenergebnis und „Neugliederung“ von Art. 32 DS-GVO*

Nach Auslegung des Art. 32 Abs. 2 DS-GVO i.V.m. Art. 32 Abs. 1 DS-GVO sind die Angemessenheitskriterien des Art. 32 Abs. 1 DS-GVO ein Teil des Art. 32 Abs. 2 DS-GVO, wonach das angemessene Schutzniveau zu bestimmen ist. Die Kriterien des ersten Absatzes ergänzen die erste, nicht abschließende Aufzählung des Art. 32 Abs. 2 DS-GVO und sind damit insgesamt bei der Bestimmung des angemessenen Schutzniveaus zu berücksichtigen. Grafisch lässt sich dies wie folgt darstellen:

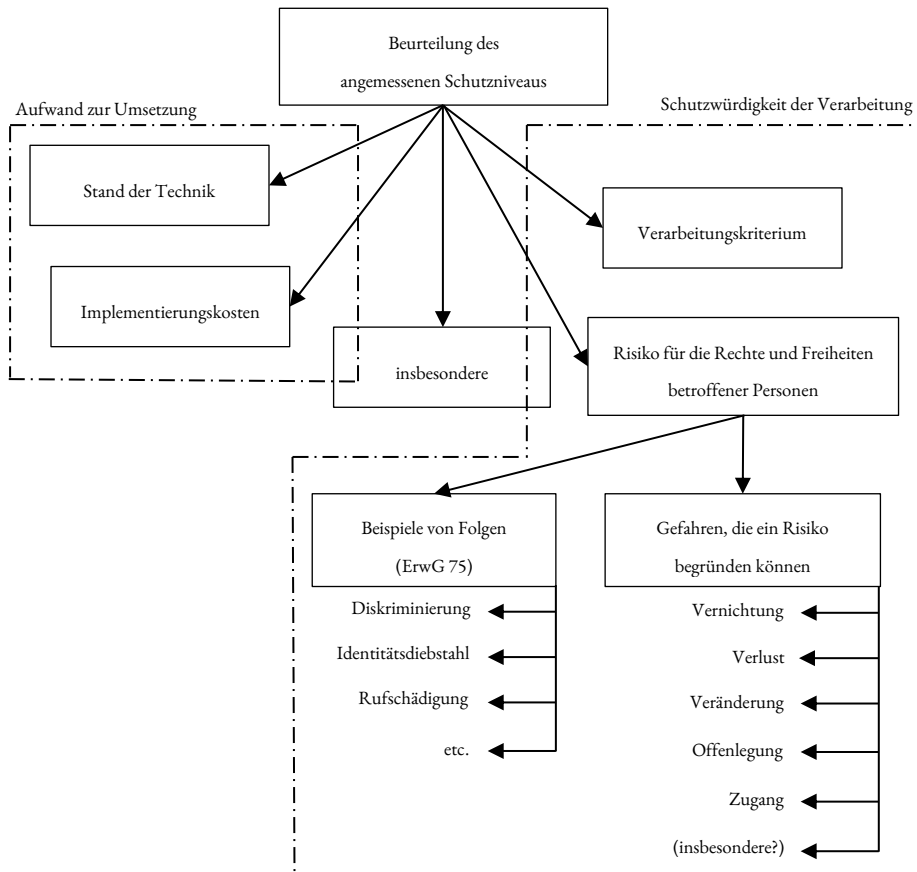


Abb. 4: Bestimmung des angemessenen Schutzniveaus (eigene, die Abb. 2 ergänzende Darstellung)

Gleichzeitig haben die Untersuchungen hier und an bereits früherer Stelle der Arbeit ergeben, dass Art. 32 DS-GVO ein sehr komplexes Zusammenspiel zwischen den ersten beiden Absätzen aufweist. Aufgrund missglückter Formulierungen und teils unsystematischen Strukturen schafft es Art. 32 DS-GVO nicht, den Regelungsgehalt für den Rechtsanwender klar wiederzugeben. Die Folge liegt vor allem in einem „falschen“ Verständnis davon, was Art. 32 DS-GVO regelt und wie diese Regelung aufgebaut ist. Um dem entgegenzuwirken,

soll daher nachfolgend versucht werden, auf Basis der Ergebnisse der durchgeführten Auslegung, eine „Neugliederung“ des Art. 32 DS-GVO vorzunehmen.

Art. 32 DS-GVO (neu): Sicherheit der Verarbeitung

- (1) *Verantwortliche und Auftragsverarbeiter treffen technische und organisatorische Maßnahmen, um während der Verarbeitung personenbezogener Daten ein angemessenes Sicherheitsniveau vor dem Eintritt und den Folgen eines personal data breach zu gewährleisten.<sup>69</sup>*
- (2) *Bei der Beurteilung des angemessenen Sicherheitsniveaus sind insbesondere der Stand der Technik, die Implementierungskosten, die verarbeitungsspezifischen Modalitäten (wie die Art, der Umfang, die Umstände und der Zweck der Verarbeitung) und das aus einem personal data breach resultierende Risiko für die Rechte und Freiheiten betroffener Personen zu berücksichtigen.<sup>70</sup>*
- (3) *<sup>1</sup>Das angemessene Sicherheitsniveau ist über die gesamte Dauer der Verarbeitung zu gewährleisten. <sup>2</sup>Verantwortliche und Auftragsverarbeiter haben daher ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des angemessenen Sicherheitsniveaus und der Wirksamkeit der technischen und organisatorischen Maßnahmen einzuführen. <sup>3</sup>Das Verfahren sollte unter Berücksichtigung des Risikos für die Rechte und Freiheiten betroffener Personen ausgestaltet sein.<sup>71</sup>*

---

<sup>69</sup> Art. 32 Abs. 1 DS-GVO (neu) stellt nun ausdrücklich auf den Schutz vor einem personal data breach ab und ersetzt damit die abstrakte (Haupt-)Anknüpfung an das Risiko für die Rechte und Freiheiten natürlicher/betroffener Personen. Die „Hilfestellung“, was von den Maßnahmen umfasst sein kann, wurde hier ersatzlos gestrichen und sollte durch den klaren Bezug auf den personal data breach nicht erforderlich sein.

<sup>70</sup> Die Abwägung im Rahmen der Angemessenheit ist nun einheitlich in Art. 32 Abs. 2 DS-GVO (neu) geregelt. Die Aufzählung ist unter Berücksichtigung des Gebots der Verhältnismäßigkeit als (weiterhin) nicht abschließende Aufzählung der Abwägungskriterien konzipiert. Weitere Kriterien, wie die datenschutzrechtliche Bewertung (siehe sogleich) ergänzen damit die Aufzählung.

<sup>71</sup> Die Einführung eines Überprüfungsverfahrens wurde aus der Liste möglicher Maßnahmen bzw. den hiermit verfolgten Zielen des Art. 32 Abs. 1 Hs. 2 DS-GVO in einen eigenen Absatz aufgenommen. Zwar stellt die Überprüfung eine Selbstverständlichkeit dar, doch sollten

- (4) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.<sup>72</sup>

### 3. Die datenschutzrechtliche Bewertung von TOM als unbenannter Abwägungstatbestand durch Auslegung der offenen Aufzählung

Nach der hier vertretenen Ansicht zählt Art. 32 DS-GVO die Kriterien für die Abwägung eines angemessenen Schutzniveaus nicht abschließend auf. Damit besteht methodisch grds. ein Instrument die Abwägungskriterien zur Bestimmung des angemessenen Schutzniveaus im Wege der Auslegung um ein zusätzliches Kriterium zu erweitern. Zu klären bleibt noch, ob die datenschutzrechtliche Bewertung von TOM auch ein Teil dieser Aufzählung darstellt. Die Gründe für eine Berücksichtigung der datenschutzrechtlichen Bewertung von TOM sowie die Kompatibilität eines solchen Kriteriums innerhalb der bestehenden Angemessenheitsprüfung wurden bereits ausführlich dargelegt.<sup>73</sup> Beides spricht dafür, ein entsprechendes Kriterium in die Angemessenheitsprüfung aufzunehmen und somit die nicht abschließende Aufzählung der Angemessenheitskriterien dahingehend zu erweitern.

---

Datenverarbeiter gesondert verpflichtet sein, ein Überprüfungsverfahren einzuführen. Im Gegensatz zu Art. 32 Abs. 1 Hs. 2 DS-GVO könnte man hier – ausgehend vom Wortlaut – eine Verschärfung zur bisherigen Regelung sehen, da ein solches Überprüfungsverfahren nun stets verpflichtend ist. Allerdings dürfte auch nach der bisherigen Regelung ein solches Verfahren wohl der Grundfall sein. Die Streitfrage dürfte vielmehr darin liegen, wie ausführlich dieses Überprüfungsverfahren ausgestaltet sein muss. Hierzu wurde daher der Satz 3 eingefügt, der dies anhand des Risikos bemessen will. Siehe zur Ausrichtung der Überprüfung anhand des Risikos nach „aktueller“ Rechtslage: Statt vieler zunächst Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 30, siehe ausführlich auch: Kap. 12, F. *Überprüfung des angemessenen Schutzniveaus* und dort insb. die Nachweise in Fn. 38.

<sup>72</sup> Art. 32 Abs. 3 DS-GVO wurde unverändert in Art. 32 Abs. 4 DS-GVO (neu) aufgenommen.

<sup>73</sup> Siehe hierzu: Kap. 2 Datenverarbeitende TOM im Regelungsbereich zwischen Art. 32 und Art. 6 DS-GVO und Kap. 7, C., I. *Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO.*

Ein letztes Hindernis verbleibt noch. Zwar wurde festgestellt, dass Art. 32 Abs. 2 DS-GVO die Kriterien für die Bestimmung des angemessenen Schutzniveaus nach Art. 32 Abs. 1 DS-GVO nicht abschließend aufzählt.<sup>74</sup> Ferner konnte gezeigt werden, dass die Kriterien für die Angemessenheit des Schutzniveaus nach Art. 32 Abs. 1 DS-GVO in die (erste) offene Aufzählung nach Art. 32 Abs. 2 DS-GVO zu integrieren sind.<sup>75</sup> Fraglich bleibt aber noch, ob nach dieser Integration die Aufzählung des Art. 32 Abs. 2 DS-GVO weiterhin offen für weitere Kriterien bleibt oder ob durch die Integration der Abwägungskriterien nach Art. 32 Abs. 1 DS-GVO die Aufzählung „vervollständigt“ wurde.

Eine klare „Vervollständigung“ einer offenen Aufzählung gibt es für sich genommen nicht. Entscheidet sich der Gesetzgeber für eine nicht abschließende Aufzählung, dann sind eventuell weitere Kriterien als solche aus dem Wortlaut nicht erkennbar. Ob weitere Kriterien unter eine nicht abschließende Aufzählung fallen, entscheidet sich nicht nach quantitativen Aspekten, sondern nach qualitativen. Im Wege der Auslegung ist demnach zu untersuchen, welche weiteren Kriterien der Gesetzgeber unter die nicht abschließende Aufzählung fassen wollte. In diesem Zusammenhang könnte aber die besondere Struktur des Art. 32 DS-GVO zu beachten sein.

Bei der Auslegung der weiteren Kriterien für die erste Aufzählung nach Art. 32 Abs. 2 DS-GVO ist der Frage nachzugehen, ob der Gesetzgeber mit seiner nicht abschließenden Aufzählung lediglich auf die weiteren Kriterien in Art. 32 Abs. 1 DS-GVO „verweisen“ wollte. In diesem Fall wäre für ein ergänzendes Kriterium – wie dem der datenschutzrechtlichen Bewertung von TOM – kein Platz. Die nicht abschließende Aufzählung würde dann durch die Kriterien nach Art. 32 Abs. 1 DS-GVO „vervollständigt“.

Anhaltspunkte hierfür liefert ausgehend von der bisherigen Untersuchung die Verordnung nicht. Einzig aus der Funktion der Angemessenheitsprüfung und ihrer Ziele lassen sich entsprechende Erkenntnisse gewinnen. Das – schon mehrfach angesprochene – Gebot der Verhältnismäßigkeit, das der Angemessenheitsprüfung zugrunde liegt, spricht für eine umfassende Abwägung sämtlicher, relevanter Faktoren bei der Bestimmung des angemessenen Schutzniveaus. Daher wäre es auch nachvollziehbar, dass sich der Gesetzgeber aus diesem

---

<sup>74</sup> Siehe hierzu: Kap. 7, C., II., 2., c), bb) *Die erste Aufzählung des Art. 32 Abs. 2 DS-GVO als echte, offene Aufzählung.*

<sup>75</sup> Siehe hierzu: Kap. 7, C., II., 2., c), ee) *Eigene Lösung.*

Grund für eine offene Aufzählung entschieden hat, da es andernfalls kaum möglich wäre, alle relevanten Kriterien abschließend aufzuzählen. Speziell im Zusammenhang mit dem Kriterium der datenschutzrechtlichen Bewertung von TOM ist ergänzend noch einmal darauf hinzuweisen, dass eine Berücksichtigung im Rahmen der Angemessenheit fast schon zwingend ist.<sup>76</sup>

Insgesamt sollte man daher zu dem Schluss kommen, dass die offene Aufzählung nach Art. 32 Abs. 2 DS-GVO nicht durch die Kriterien nach Absatz 1 „vervollständigt“ wird und somit Platz für weitere Kriterien lässt. Ein Kriterium muss hierbei die datenschutzrechtliche Bewertung von TOM sein.

Grafisch lässt sich dies also wie folgt darstellen:

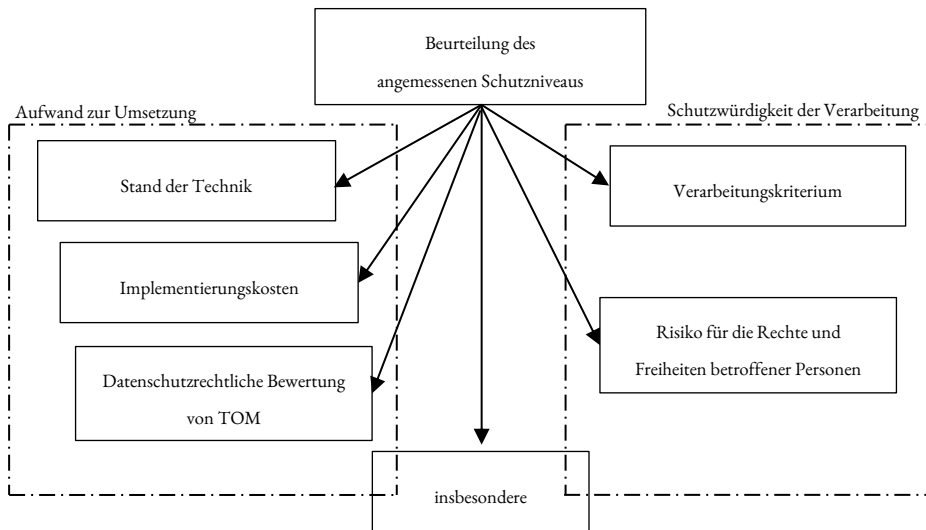


Abb. 5: Bestimmung des angemessenen Schutzniveaus unter Berücksichtigung datenverarbeitender TOM (eigene, die Abb. 2 und 4 ergänzende, aber z.T. gekürzte Darstellung)

Welche weiteren Kriterien von der Angemessenheitsprüfung noch umfasst sein könnten, ist für die weitere Untersuchung nicht relevant. Denkbar wären

<sup>76</sup> Siehe bereits: Kap. 7, C., I., 3. Die teleologische Rechtfertigung für ein eigenes Abwägungskriterium.



vielleicht noch verhaltens-psychologische Aspekte, wie die Akzeptanz bestimmter TOM, die in die Bewertung der Angemessenheit des Schutzniveaus mit aufgenommen werden könnten.

#### *4. Alternative: Die datenschutzrechtliche Bewertung von TOM als unbenannter Abwägungstatbestand im Wege einer teleologischen Reduktion*

Nach deutschem Verständnis kann der hier vorgeschlagene, methodische Weg, ein unbenanntes Abwägungskriterium im Wege der Auslegung herzuleiten, als etwas weit aufgefasst werden. Der EuGH differenziert nicht klar zwischen der „einfachen“ Auslegung und einer Rechtsfortbildung, sondern fasst beides unter die „*interprétation*“.<sup>77</sup> Dadurch stellt auch der Wortlaut – anders als verbreitet nach der deutschen Rechtsmethodik –<sup>78</sup> nicht die Grenze der Auslegung dar.<sup>79</sup> Zwar ist nach hier vertretener Ansicht der vorgeschlagene Lösungsweg weiterhin mit dem Wortlaut von Art. 32 DS-GVO vereinbar. Nichtsdestotrotz greift die Lösung deutlich in die Regelungstechnik des Art. 32 DS-GVO ein. Dabei stützt sich die Lösung vor allem auf das Telos der Vorschrift. Nach hier vertretener Ansicht ist dieser Eingriff daher gerechtfertigt und dem angemessenen

---

<sup>77</sup> Statt vieler Riesenhuber/Neuner, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 2. Siehe für weitere Nachweise: Kap. 7, C., II., 1. *Darstellung möglicher Lösungswege* und dort die Fn. 80.

<sup>78</sup> Siehe zum Wortlaut als Grenze zwischen Auslegung und Rechtsfortbildung in der deutschen Rechtsmethodik: *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, S. 366; *Bydlinski*, Juristische Methodenlehre und Rechtsbegriffe, 2. Aufl. 1991, S. 441, 467 ff.; *Canaris*, Die Feststellung von Lücken im Gesetz, 2. Aufl. 1983, S. 19 ff.; *Zippelius*, Juristische Methodenlehre, 12. Aufl. 2021, S. 39, 51; kritisch *Wank*, Juristische Methodenlehre, 2020, § 15, Rn. 15 ff.; ebenfalls kritisch *Reimer*, Juristische Methodenlehre, 2. Aufl. 2020, Rn. 553.

<sup>79</sup> *Höpfner/Rüthers*, AcP 209 (2009), S. 1, 10; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 15. Siehe auch *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, S. 38 f., der es bereits aufgrund der Vielfalt der verbindlichen Sprachen als schwierig ansieht, eine solche Grenze zu bestimmen und lehnt insgesamt die Unterscheidung zwischen Auslegung und Rechtsfortbildung für das Europäische Recht ab; ebenfalls ablehnend zur Unterscheidung zwischen Auslegung und Rechtsfortbildung und damit auch der Wortlautgrenze *Martens*, Methodenlehre des Unionsrechts, 2013, S. 503 f.

Schutzniveau nach Art. 32 Abs. 1 DS-GVO liegt eine umfassende Verhältnismäßigkeitsprüfung zugrunde, um die Ziele und den damit verbundenen Aufwand in ein gerechtes Verhältnis zu setzen.<sup>80</sup>

Wer – nach deutschem Rechtsverständnis – diesem Weg, einer weitreichenden Rechtsauslegung – nicht folgen wollte, müsste dennoch anerkennen, dass rechtliche Faktoren im Zusammenhang mit der Umsetzung der Sicherheit der Verarbeitung bereits bei der Definition der Anforderungen an die Sicherheit zwingend berücksichtigt werden sollten.<sup>81</sup> Gerade mit Blick auf die benannten Abwägungskriterien wäre es nicht zu rechtfertigen, diese Faktoren unberücksichtigt zu lassen. Als Alternative für den hier dargestellten, methodischen Weg müsste man dann eine Rechtsfortbildung in Betracht ziehen. Denkbar wäre hier die Schaffung eines ungeschriebenen Abwägungstatbestands mittels einer teleologischen Reduktion, der die datenschutzrechtliche Bewertung von TOM berücksichtigt.

Der Weg über eine – dem deutschen Verständnis entsprechende – teleologische Reduktion wäre zudem nicht nach der – hier entscheidenden europäischen Rechtsmethodik – ausgeschlossen. So hat der EuGH bereits das Recht so „ausgelegt“, dass es sich nach deutschem Verständnis nur um eine teleologische Reduktion handeln kann.<sup>82</sup> Ein bekanntes Beispiel für die Schaffung eines ungeschriebenen Tatbestandsmerkmals mittels einer „teleologischen Reduktion“

---

<sup>80</sup> Siehe zur Rechtfertigung für dieses Kriterium ausführlicher: Kap. 7, C., I. *Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO.*

<sup>81</sup> Siehe zur teleologischen Rechtfertigung: Kap. 7, C., I., 3. *Die teleologische Rechtfertigung für ein eigenes Abwägungskriterium.*

<sup>82</sup> Siehe allgemein zur – nach deutschem Verständnis – „teleologischen Reduktion“ im Europäischen Recht: Statt vieler EuGH, Rs. C-81/79 (Sorasio-Allo u.a./Kommission), ECLI:EU:C:1980:270 = BeckRS 2004, 73763, Rn. 15; Riesenhuber/Neuner, Europäische Methodenlehre, 4. Aufl. 2021, § 12, Rn. 38 ff. Siehe für weitere Nachweise: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle* und dort die Fn. 106.

stellt der Tatbestand der „Spürbarkeit“ sowohl einer Wettbewerbsbeschränkung<sup>83</sup> als auch ihrer Eignung den Handel zwischen den Mitgliedstaaten zu beeinträchtigen<sup>84</sup>, im europäischen Kartellrecht dar.<sup>85</sup>

Selbst wenn man den hier favorisierten Weg der Schaffung eines ungeschriebenen Abwägungstatbestands für die datenschutzrechtliche Bewertung von TOM im Wege der Auslegung der nicht abschließenden Aufzählung nach Art. 32 Abs. 2 DS-GVO nicht folgen kann, lässt sich ein entsprechendes Kriterium sonst im Rahmen einer teleologischen Reduktion begründen.

### III. Konkretisierung des ungeschriebenen Abwägungskriteriums der datenschutzrechtlichen Bewertung von TOM

Der Grund für und der wesentliche Anwendungsbereich eines Kriteriums, dass die datenschutzrechtliche Bewertung von TOM im Rahmen des angemessenen

---

<sup>83</sup> EuGH, Rs. C-5/69 (Voelk/Vervaecke), ECLI:EU:C:1969:35 = BeckRS 2004, 73207, Rn. 7; EuGH, Rs. C-260/07 (Pedro IV Servicios), ECLI:EU:C:2009:215 = EuZW 2009, S. 374, Rn. 68; EuGH, Rs. C-226/11 (Expedia), ECLI:EU:C:2012:795 = NZKart 2013, S. 111, Rn. 17; Immenga/Mestmäcker/Zimmer, Wettbewerbsrecht, 1. Bd., 6. Aufl. 2019, Art. 101 Abs. 1 AEUV, Rn. 138; Loewenheim u.a./Grave/Nyberg, Kartellrecht, 4. Aufl. 2020, Art. 101 Abs. 1 AEUV, Rn. 259; Bunte/Hengst, Kartellrecht, Bd. 2, 14. Aufl. 2022, Art. 101 AEUV, Rn. 260; MüKo Wettbewerbsrecht/Säcker/Zorn, Bd. 1, 4. Aufl. 2023, Art. 101 AEUV, Rn. 283, 288 ff., jedoch ablehnend zur dogmatischen Einordnung als ungeschriebenes Tatbestandsmerkmal und sehen hierin eine „formelle Bagatellgrenze“.

<sup>84</sup> EuGH, Rs. C-27/87 (Erau-Jacquery/La Hesbignonne), ECLI:EU:C:1988:183 = BeckRS 2004, 72822, Rn. 17; EuGH, Rs. C-306/96 (Javico/Yves Saint Laurent Parfums), ECLI:EU:C:1998:173 = EuZW 1998, S. 404, Rn. 16, 25; EuGH, Rs. C-238/05 (ASNEF-EQUIFAX und Administración del Estado), ECLI:EU:C:2006:734 = BeckRS 2006, 70910, Rn. 34; Immenga/Mestmäcker/Zimmer, Wettbewerbsrecht, 1. Bd., 6. Aufl. 2019, Art. 101 Abs. 1 AEUV, Rn. 181; Loewenheim u.a./Grave/Nyberg, Kartellrecht, 4. Aufl. 2020, Art. 101 Abs. 1 AEUV, Rn. 295; Bunte/Hengst, Kartellrecht, Bd. 2, 14. Aufl. 2022, Art. 101 AEUV, Rn. 334; MüKo Wettbewerbsrecht/Kirchhoff, Bd. 1, 4. Aufl. 2023, Art. 101 AEUV, Rn. 822.

<sup>85</sup> Konkret zur methodischen Einordnung als „teleologische Reduktion“ dieser beiden ungeschriebenen Tatbestandsmerkmale: Dannecker/Fischer-Fritsch, Das EG-Kartellrecht in der Bußgeldpraxis, 1989, S. 15, zum damaligen Art. 85 EWGV (heute Art. 101 AEUV); Terbechte, Die ungeschriebenen Tatbestandsmerkmale des europäischen Wettbewerbsrechts, 2004, S. 188 ff., zum damaligen Art. 81 EGV (heute Art. 101 AEUV); siehe auch Jung/Krebs/Stiegler/Krebs/Jung, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 174, mit allgemeinem Verweis auf das Spürbarkeitserfordernis im Kartellrecht.

Schutzniveaus berücksichtigt, wurde hier umfassend hergeleitet.<sup>86</sup> Unabhängig davon, ob man einen solchen, ungeschriebenen Abwägungstatbestand nun im Rahmen der „einfachen“ Auslegung – wie hier vertreten – oder im Wege einer teleologischen Reduktion begründet, stellt sich weiterhin die Frage, wie ein solches Kriterium nun im Detail aussehen könnte. Das Kriterium befasst sich mit den datenschutzrechtlichen Faktoren bei der späteren Umsetzung der Sicherheit der Verarbeitung. Dadurch sind im Rahmen der Angemessenheitsprüfung die datenschutzrechtlichen Anforderungen zu berücksichtigen, die die Rechtsordnung an die Implementierung von Sicherheitsmaßnahmen stellt. Bei den untersuchten datenverarbeitenden TOM wären dies insbesondere die datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten i.S.d. Art. 6 DS-GVO, die beim Einsatz dieser Sicherheitsmaßnahmen vorgenommen wird.

Das Kriterium erlaubt es insofern, die Wertungen über die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten nach Art. 6 DS-GVO im Zusammenhang der Sicherheit der Verarbeitung zu berücksichtigen, um damit den Einklang der Rechtsordnung bzw. hier des Rechtsakts zu wahren. Im Vordergrund dürften dabei die Fälle stehen, in denen Art. 6 DS-GVO die Implementierung besagter Sicherheitsmaßnahmen aufgrund ihrer Verarbeitung personenbezogener Daten verbietet, da hier der Konflikt innerhalb der Datenschutz-Grundverordnung am größten ist.

Allerdings ist darauf hinzuweisen, dass der Anwendungsbereich nicht nur auf diese Fälle begrenzt sein sollte. Vorstellbar wäre die Anwendung auch auf Sicherheitsmaßnahmen, an die Art. 6 DS-GVO bestimmte Anforderungen knüpft, ohne gleich ein finales Verbot auszusprechen. In diesen Fällen sieht das Gesetz ebenfalls einen gewissen Schutz vor dem Einsatz der Sicherheitsmaßnahmen vor, der aber noch nicht zu einem absoluten Verbot führen muss.

Dass das Kriterium der datenschutzrechtlichen Bewertung von TOM bereits dort eingreifen kann, wo es rechtliche Anforderungen an die Implementierung der Sicherheitsmaßnahmen gibt, zeigt sich auch bei einem Vergleich mit den anderen Abwägungskriterien. Das beste Beispiel liefert hier das Kriterium der Implementierungskosten. Denn Art. 32 DS-GVO macht hiermit keine Vorgaben dahingehend, ab welchem Wert Implementierungskosten zu hoch sind für die

---

<sup>86</sup> Siehe hierzu: Kap. 7, C., I. *Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO.*

Gewährleistung eines bestimmten Schutzniveaus. Vielmehr kommt es dann auf den Vergleich mit der Schutzwürdigkeit (und den weiteren Kriterien) an.

Auch dem Kriterium des Stands der Technik<sup>87</sup> sollte diese Betrachtung zugrunde liegen. In der Literatur zeigt sich hierbei aber ein abweichendes Bild. Wie bereits dargelegt, wird in der Literatur sehr häufig der „Stand der Technik“ von anderen Begriffen aus diesem Bereich, wie den „(allgemein anerkannten) Regeln der Technik“ und dem „Stand der Wissenschaft und Technik“, abgegrenzt.<sup>88</sup> Eine solche Abgrenzung hat dann aber unmittelbar zur Folge, dass dem Stand der Technik damit auch eine inhaltliche Abgrenzung vorzunehmen ist. So wird vertreten, dass die Datenverarbeiter „nur“ dazu verpflichtet sind, Maßnahmen nach dem Stand der Technik zu berücksichtigen und keine höheren Standards, aber auch keinen niedrigeren Standard zu implementieren.<sup>89</sup>

Diese Auffassung ist mit Blick auf die Anforderungen des Art. 32 DS-GVO allerdings problematisch. Denn der Begriff Stand der Technik oder vielleicht besser seine Rolle im Rahmen der Abwägung dürfte vielmehr weiter gefasst sein. Denn wie Art. 32 Abs. 1 DS-GVO einleitend hervorhebt, ist u.a. der Stand der Technik innerhalb der Abwägung (nur) zu berücksichtigen („*Unter Berücksichtigung*“<sup>90</sup>). Damit beschränkt sich Art. 32 DS-GVO nicht auf den „Stand der Technik“ (wie auch immer dieser konkret zu bestimmen und ggf. abzugrenzen ist).<sup>91</sup> Dies gilt sowohl hinsichtlich der Abgrenzung zu einem höheren wie auch

---

<sup>87</sup> Siehe zu diesem Kriterium bereits die Ausführungen unter: Kap. 7, B., I. *Stand der Technik*.

<sup>88</sup> Siehe hierzu: Kap. 7, B., I. *Stand der Technik*.

<sup>89</sup> So wohl Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 10; in diese Richtung argumentiert ebenfalls (zurückhaltend) DatKomm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 20; Forgó/Helfrich/Schneider/Schmitz/v. Dall’Armi, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 1, Rn. 47; wohl auch Gärtner/Selzer, DuD 2023, S. 289, 291, die von „dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen“ sprechen; ähnlich Schläger/Thode/Schläger, Hdb. Datenschutz und IT-Sicherheit, 2. Aufl. 2022, Kapitel G, Rn. 11 f.

<sup>90</sup> Englisch: „*Taking into account*“, Französisch: „*Compte tenu*“, Spanisch: „*Teniendo en cuenta*“, Italienisch: „*Tenendo conto*“, Niederländisch: „*Rekening houdend*“.

<sup>91</sup> Gola/Heckmann/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 14; Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 24; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 56; Bartels/Backer, DuD 2018, S. 214, 216 ff.; Johannes/Geminn, InTeR 2021, S. 140, 143; vgl. auch Piltz, K&R 2016, S. 709, 714; Seufert, ZD 2023, S. 256, 258, wohl gemeinsam zu Art. 25 und 32 DS-GVO; siehe auch Knopp, DuD 2017, S. 663, 666, der

einem niedrigeren Standard. Ob Datenverarbeiter letztlich dazu verpflichtet werden, TOM zu implementieren, die dem Stand der Technik, einem höheren oder einem niedrigeren Standard entsprechen, richtet sich einzig nach der Angemessenheitsprüfung und der vorausgegangenen Prüfung der Schutzwürdigkeit, ausgehend vom bestehenden Risiko.<sup>92</sup>

Andernfalls könnte man nur schwer erklären, dass bei einer hoch riskanten Verarbeitung die Pflichten des Datenverarbeiters an der Grenze des Stands der Technik halt machen sollten, obwohl alle anderen Kriterien der Angemessenheit für ein höheres Schutzniveau plädieren. Etwas Ähnliches zeigt sich auch in die entgegengesetzte Richtung, wenn das Risiko derart gering ist, dass ein einfacherer und vielleicht unter dem Stand der Technik liegender Schutz vollkommen ausreichen würde.

Bei der Ausgestaltung des Kriteriums datenschutzrechtlicher Bewertung von TOM zeigt sich etwas Ähnliches. Es kommt auch hier nicht zwingend auf ein datenschutzrechtliches Verbot von Sicherheitsmaßnahmen an. Vielmehr muss auch hier gefragt werden, ob allgemein die rechtlichen Anforderungen an die Sicherheitsmaßnahmen im Vergleich zur Schutzwürdigkeit der Verarbeitung (und der anderen Kriterien) verhältnismäßig sind.

## D. Zwischenergebnis

Die Kriterien zur Bestimmung eines angemessenen Schutzniveaus werden in Art. 32 DS-GVO nur beispielhaft aufgezählt. Es handelt sich insofern um eine

---

herausstellt, dass es darauf ankommt, die Ziele zu erreichen und dass der „Stand der Technik“ nicht das einzige Kriterium für die Angemessenheit ist (allerdings nicht konkret zu Art. 32 DS-GVO).

<sup>92</sup> *Johannes/Geminn*, InTeR 2021, S. 140, 143, gehen allerdings vom Grundsatz aus, dass der Stand der Technik einzuhalten ist und nur davon abgewichen werden kann, wenn die Abwägung etwas anderes ergibt; ähnlich auch *Simitis/Hornung/Spiecker gen. Döhmman/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 24, spricht davon, dass es sich regelmäßig um eine „untere Grenze“ handelt; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 56, der ausdrücklich nur auf die Möglichkeit der Unterschreitung in Ausnahmesituationen abstellt; siehe auch *Seufert*, ZD 2023, S. 256, 258, wohl gemeinsam zu Art. 25 und 32 DS-GVO, die ebenfalls auf die Möglichkeit verweist, den Stand der Technik „begründet zu unterschreiten“.

umfassende Verhältnismäßigkeitsprüfung. Rechtliche Vorgaben an die Sicherheitsmaßnahmen, die der Umsetzung der Sicherheit der Verarbeitung dienen, können es den Datenverarbeitern erschweren, die Sicherheit der Verarbeitung zu gewährleisten. Ähnlich wie die Kriterien des Stands der Technik und den Implementierungskosten müssen neben diese tatsächlichen bzw. wirtschaftlichen Faktoren konsequenterweise auch rechtliche Faktoren bei der Bestimmung des angemessenen Schutzniveaus berücksichtigt werden. Die Verhältnismäßigkeitsprüfung ist daher um ein Kriterium der datenschutzrechtlichen Bewertung von TOM zu „ergänzen“. Den methodischen Weg hierfür bildet ein ungeschriebenes Tatbestandsmerkmal, das sich im Wege der Auslegung aus der nicht abschließenden Auflistung der Abwägungskriterien herleitet.

Als Abwägungskriterium erfasst es aber nicht nur die klaren Fälle, in denen ein datenschutzrechtliches Verbot der Implementierung von Sicherheitsmaßnahmen der Umsetzung der Sicherheit der Verarbeitung entgegenstehen könnte. Auch in dem Bereich zwischen „erlaubten“ und „verbotenen“ Maßnahmen kann das Kriterium einen Beitrag zur Angemessenheit des Schutzniveaus leisten. Dies könnte vor allem dort wichtig sein, wo rechtliche Anforderungen nicht unbedingt ein Verbot für die Implementierung von Sicherheitsmaßnahmen aussprechen, aber rechtliche „Vorbehalte“ oder „Auflagen“ bleiben.

Bei datenverarbeitenden TOM stellt die Datenschutz-Grundverordnung in Art. 6 DS-GVO Anforderungen an die, den Maßnahmen zugrundeliegende Verarbeitung personenbezogener Daten. Diese Anforderungen ließen sich sodann im Rahmen des „neuen“ Abwägungskriteriums bei der Bestimmung des angemessenen Schutzniveaus berücksichtigen. Da das Kriterium vorrangig den Aufwand für die Umsetzung adressiert, kann es als eine Art „Gegengewicht“ für das vorab zu bestimmende Risiko dienen und, gerade im Fall von datenschutzrechtswidrigen Sicherheitsmaßnahmen, letztlich zu einer Absenkung des Schutzniveaus führen, wenn eine Umsetzung andernfalls nicht verhältnismäßig wäre. Auf der Seite der Sicherheit der Verarbeitung ließe sich somit der beschriebene Konflikt im 1. Teil dieser Arbeit entschärfen.

Denn (1) werden Datenverarbeiter „faktisch“ nicht dazu gezwungen, datenschutzwidrige Sicherheitsmaßnahmen zu implementieren. Eine Herabsetzung des angemessenen Schutzniveaus durch das Kriterium der datenschutzrechtlichen Bewertung von TOM würde verhindern, dass sich ein Schutzniveau einpendelt, das nur mittels verbotener Sicherheitsmaßnahmen umgesetzt werden könnte.

(2) wären Datenverarbeiter vor einer „fiktiven“ Angemessenheitsprüfung geschützt, die vorab sämtliche, denkbaren und wirtschaftlich angemessenen Sicherheitsmaßnahmen bei der Bestimmung des angemessenen Schutzniveaus zugrunde legt, die aber anschließend aufgrund rechtlicher Hindernisse nicht umgesetzt werden können. Gleichzeitig wahrt die Lösung hier die Trennung zwischen der Sicherheit der Verarbeitung und den Sicherheitsmaßnahmen, so dass das Verbot einzelner Sicherheitsmaßnahmen nicht zwangsweise zu einer Absenkung des Schutzniveaus führt, wenn es andere, verhältnismäßige Alternativen gibt.



## Teil 3

### Die Rechtmäßigkeit datenverarbeitender TOM

Im Rahmen der Angemessenheit des Schutzniveaus i.S.d. Art. 32 Abs. 1 DSGVO lässt sich die datenschutzrechtliche Bewertung von technischen und organisatorischen Maßnahmen berücksichtigen und entscheidet demnach mitunter über das geforderte Schutzniveau zur Gewährleistung der Sicherheit der Verarbeitung.<sup>1</sup> Im Fall der datenverarbeitenden TOM stellen sich Fragen ihrer datenschutzrechtlichen Bewertung hinsichtlich der Rechtmäßigkeit der ihnen zugrundeliegenden Verarbeitung personenbezogener Daten. Hier ist nochmal auf die Prämisse hinzuweisen, nach der diese Datenverarbeitung essenziell für die Funktion der Maßnahmen zur Gewährleistung der Sicherheit nach Art. 32 DSGVO ist.<sup>2</sup>

Nachfolgend ist daher zunächst zu untersuchen, welche Anforderungen das Datenschutzrecht an die rechtmäßige Verarbeitung personenbezogener Daten stellt, um diese anschließend im Lichte der datenverarbeitenden TOM zu bewerten.

---

<sup>1</sup> Siehe hierzu: Kap. 7, D. *Zwischenergebnis*.

<sup>2</sup> Siehe zu dieser Prämisse: Kap. 1, B. *Definition*.



## Kapitel 8

# Das System der Rechtmäßigkeit von Datenverarbeitungen

### A. Die Notwendigkeit einer Rechtsgrundlage

Wie bereits im 1. Teil dargelegt, bedarf nach dem europäischen Datenschutzrecht jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage.<sup>1</sup> Die Datenschutz-Grundverordnung führt die Rechtsgrundlagen für eine rechtmäßige Datenverarbeitung zentral<sup>2</sup> in Art. 6 Abs. 1 UAbs.<sup>3</sup> 1 DS-GVO auf.<sup>4</sup> Die

---

<sup>1</sup> Siehe hierzu: Kap. 2, A., II. *Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO.*

<sup>2</sup> Für besondere Datenkategorien ist auch Art. 9 DS-GVO zu beachten. Aufgrund systematischer Überschneidungen ist das Verhältnis zwischen Art. 9 und Art. 6 DS-GVO im Detail noch umstritten. Siehe hierzu die Ausführungen oben: Kap. 3, C., V. *Beschränkung auf die Rechtmäßigkeit der Verarbeitung nach Art. 6 DS-GVO* gemeinsam mit der Einschränkung auf „gewöhnliche“ personenbezogene Daten und damit auf Art. 6 DS-GVO in dieser Arbeit.

<sup>3</sup> Die Datenschutz-Grundverordnung zitiert Art. 6 DS-GVO nicht einheitlich. So spricht sie am Ende von Art. 6 Abs. 1 DS-GVO von „*Unterabsatz 1 Buchstabe f*“, dann u.a. aber in Art. 6 Abs. 2 DS-GVO von „*Absatz 1 Buchstabe e*“. Nachfolgend wird die Zitierweise mit Unterabsatz verwendet.

<sup>4</sup> Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 1; DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 1 f.; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 1 f.; Heinzke/Engel, ZD 2020, S. 189, 189.

dort aufgelisteten Rechtsgrundlagen sind grds.<sup>5</sup> abschließend.<sup>6</sup> Art. 6 Abs. 1 UAbs. 1 DS-GVO listet insgesamt sechs Rechtsgrundlagen auf, auf die eine Datenverarbeitung gestützt werden kann. Die Verarbeitung personenbezogener Daten ist danach rechtmäßig, wenn sie:

- mit Einwilligung der betroffenen Person erfolgt (lit. a)),
- erforderlich ist für die Erfüllung eines Vertrages mit der betroffenen Person oder erforderlich ist für die Durchführung vorvertraglicher Maßnahmen auf Initiative der betroffenen Person (lit. b)),
- erforderlich ist für die Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen (lit. c)),

---

<sup>5</sup> Einige Rechtsgrundlagen weisen eine Offenheit auf, die die Einordnung als abschließende Aufzählung relativiert. Ausführlicher wird diese Systematik in Kap. 8, C., III., 2. *Verwirklichung der Abwägung* behandelt. Ähnlich kritisch zum (vermeintlich) abschließenden Charakter: BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 22; Paal/Pauly/*Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 1; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 2, der zudem auf Regelungen außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung verweist; siehe auch Jahnel/*Jahnel*, DSGVO, 2021, Art. 6 DS-GVO, Rn. 4. Siehe auch Jandt/Steidle/*Wilmer*, Datenschutz im Internet, 2018, B. II., Rn. 24, der insb. von einer „Durchbrechung der abschließenden Regelung“ durch Vorschriften i.S.d. Art. 6 Abs. 2, 3 DS-GVO spricht.

<sup>6</sup> EuGH, Rs. C-439/19 (Latvijas Republikas Saeima ([Points de pénalité]), ECLI:EU:C:2021:504 = BeckRS 2021, 15289, Rn. 99; EuGH, Urteil v. 08.12.2022, Rs. C-180/21 (Inspektor v Inspektorata kam Visshia sadeben savet [Finalités du traitement de données - Enquête pénale]), ECLI:EU:C:2022:967 = BeckRS 2022, 34896, Rn. 83; EuGH, Rs. C-252/21 (Meta Platforms u.a. [Conditions générales d'utilisation d'un réseau social]), ECLI:EU:C:2023:537 = GRUR 2023, S. 1131, Rn. 90; Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 4; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 1a; Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 1; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 4; Kuner/Bygrave/*Docksey/Kotschy*, GDPR, 2020, p. 325, 329; Spindler/Schuster/*Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 2. So auch die Auffassung des EuGH zur weitgehend inhaltsgleichen Vorgängervorschrift des Art. 7 DS-RL: EuGH, verb. Rs. C-468/10, C-469/10 (ASNEF), ECLI:EU:C:2011:777 = EuZW 2012, S. 37, Rn. 30; EuGH, Rs. C-582/14 (Breyer), ECLI:EU:C:2016:779 = NJW 2016, S. 3579, Rn. 57.

- erforderlich ist, um lebenswichtige Interessen einer natürlichen Person zu schützen (lit. d)),
- erforderlich ist für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde (lit. e)) oder
- erforderlich ist zur Wahrung eines berechtigten Interesses, sofern die Interessen und Grundrechte der betroffenen Person nicht überwiegen (lit. f))

## B. Ausrichtung am Zweck der Verarbeitung

Welche Rechtsgrundlagen für eine Verarbeitung personenbezogener Daten Anwendung finden können, richtet sich dabei nach dem Zweck der Verarbeitung.<sup>7</sup>

### I. Zweck der Verarbeitung

Der Verarbeitungszweck nimmt eine besondere Stellung im europäischen Datenschutzrecht ein.<sup>8</sup> Viele Vorschriften verweisen auf den Zweck der Verarbeitung und nehmen diesen als Bezugspunkt an. Wie der Wortlaut bereits nahelegt,

---

<sup>7</sup> Gola/Heckmann/Pötters, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 14; Ziegenhorn/Schulz-Große, ZD 2023, S. 581, 582 f.; BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 13; siehe auch Dammann, ZD 2016, S. 307, 311, wonach „[d]ie Zweckbestimmung [...] notwendiger Bestandteil jeder Rechtsgrundlage [ist]“.

<sup>8</sup> BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 13, „beherrschende Konstruktionsprinzip des Datenschutzrechts“; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 5 DS-GVO, Rn. 23, „Dreh- und Angelpunkt“; Dammann, ZD 2016, S. 307, 311; ähnlich DatKomm/Hötzendorfer/Tschobl/Kastelitz, Stand: 76. EL. 2023, Art. 5 DS-GVO (Stand: Juli 2020), Rn. 21. Siehe auch zur besonderen Bedeutung des Zweckbindungsgrundsatz (hierzu auch noch sogleich) im Datenschutzrecht: Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 397, „der zentrale datenschutzrechtliche Grundsatz“; ähnlich Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 3, Rn. 60; auch Chibanguza/Kuß/Steeger/Steeger/Kuß, Künstliche Intelligenz, 2022, § 2, C., Rn. 56; Knyrim/Haidinger, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.7, „zentrales Element des europäischen Datenschutzrechts“; ähnlich Culik/Döpke, ZD 2017, S. 226, 227; Kuner/Bygrave/Docksey/de Terwangne, GDPR, 2020, p. 315, „cornerstone of data protection“.

werden mit dem „Zweck“<sup>9</sup> die Beweggründe für die Verarbeitung personenbezogener Daten ausgedrückt.<sup>10</sup>

In diesem Zusammenhang spielt auch der Grundsatz der sog. „Zweckbindung“<sup>11</sup> nach Art. 5 Abs. 1 lit. b) DS-GVO eine besondere Bedeutung. Nach diesem Grundsatz dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden, Art. 5 Abs. 1 lit. b) Hs. 1 DS-GVO. Ferner dürfen personenbezogene Daten nicht zu anderen, als den ursprünglichen Zwecken weiterverarbeitet werden, wenn diese mit den ursprünglichen Zwecken unvereinbar sind, Art. 5 Abs. 1 lit. b) Hs. 2 DS-GVO.

---

<sup>9</sup> Englisch: „purpose“, Französisch: „finalité“, Spanisch: „finalidad“, Italienisch: „finalità“, Niederländisch: „doeleinde“.

<sup>10</sup> Siehe auch Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 5 DS-GVO, Rn. 8, „Verarbeitungsintention“; Freund u.a./Schmidt, DSGVO, 2023, Art. 5 DS-GVO, Rn. 29, „besondere Grund“ der Verarbeitung, mit Verweis auf Artikel-29-Gruppe, WP 217, S. 24, „specific reason“; vgl. Simitis/Hornung/Spiecker gen. Döhmann/Roßnagel, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 68, als „Beschreibung des Zustands, der [...] erreicht werden soll“ und „das Ziel und den Grund benennt“ u.a. mit Verweis auf Hoffmann, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes, 1991, S. 83; ähnlich Ziegenhorn/Schulz-Große, ZD 2023, S. 581, 582. Siehe auch Feiler/Forgó, EU-DSGVO und DSGVO, 2. Aufl. 2022, Art. 4 DS-GVO, Rn. 14, „Bezeichnung [...] des Geschäftsprozesses [...] für welchen die personenbezogenen Daten verarbeitet werden“.

<sup>11</sup> Englisch: „purpose limitation“, Französisch: „limitation des finalités“, Spanisch: „limitación de la finalidad“, Italienisch: „limitazione della finalit “, Niederländisch: „doelbinding“.

Der Zweckbindungsgrundsatz regelt damit zwei wesentliche Elemente.<sup>12</sup> Als Ausgangspunkt schreibt er vor, dass vor der erstmaligen Verarbeitung (Erhebung)<sup>13</sup> bereits ein eindeutiger und legitimer Zweck für die Verarbeitung festgelegt sein muss.<sup>14</sup> Darauf folgt anschließend, dass eine Verarbeitung grds. an den Zweck der Erhebung gebunden ist und eine Weiterverarbeitung zu anderen Zwecken eingeschränkt ist.<sup>15</sup> Bei dem zweiten Aspekt handelt es sich um die eigentliche *Zweckbindung*, wie es die deutsche Sprachfassung für den gesamten Art. 5 Abs. 1 lit. b) DS-GVO beschreibt.<sup>16</sup> Andere Sprachfassungen sprechen

---

<sup>12</sup> BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 12; *Spies*, ZD 2022, S. 75, 76 f.; *Culik/Döpke*, ZD 2017, S. 226, 227; *Monreal*, ZD 2016, S. 507, 509; *DatKomm/Hötzendorfer/Tschohl/Kastelitz*, Stand: 76. EL. 2023, Art. 5 DS-GVO (Stand: Juli 2020), Rn. 20; *Specht/Mantz/Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 84; *Sydow/Marsch/Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 19, spricht von „*Erhebungsverbot*“ und „*Weiterverarbeitungs-verbot*“; *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 582, sprechen von „*zwei Teil-Grundsätzen*“; ähnlich *Schantz/Wolff/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 400, „*zwei Untergrundsätze*“.

<sup>13</sup> Zur „*Erhebung*“ als erstmalige Verarbeitung: *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 582; siehe auch *Kühling/Buchner/Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 4 Nr. 2 DS-GVO, Rn. 21, „*erstmalig in den Verfügungsbereich des Verantwortlichen gelangen*“; a.A. wohl *Taeger/Gabel/Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 71, wonach es unerheblich sein soll, ob der Verantwortliche zuvor bereits über die Daten verfügte.

<sup>14</sup> Vgl. zum Zeitpunkt der Festlegung: BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 14; *Gola/Heckmann/Pötters*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 17; *Ehmann/Selmayr/Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 13; *Knyrim/Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.7; *Specht/Mantz/Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 85; *Spies*, ZD 2022, S. 75, 76; *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 583.

<sup>15</sup> BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 19; *Knyrim/Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.7; *Gola/Heckmann/Pötters*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 18 f.; *Ehmann/Selmayr/Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 16; *Schantz*, NJW 2016, S. 1841, 1844.

<sup>16</sup> Daher wird bei dem zweiten Aspekt auch von der „*Zweckbindung i.e.S.*“ gesprochen: BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November), Rn. 12, 22; *Spies*, ZD 2022, S. 75, 77; *Culik/Döpke*, ZD 2017, S. 226, 227 f.; *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 584; *Bronner/Wiedemann*, ZD 2023, S. 77, 81; siehe auch

bei dem Grundsatz nach Art. 5 Abs. 1 lit. b) DS-GVO eher von der „Zweckbeschränkung“<sup>17</sup>.<sup>18</sup> Von den untersuchten Sprachfassungen dürfte nur die niederländische Fassung eher in Richtung des deutschen Wortlauts zu übersetzen sein (Niederländisch: „doelbinding“).

Mit dem Zweckbindungsgrundsatz soll gerade verhindert werden, dass ohne einen bereits festgelegten Grund, Daten auf Vorrat<sup>19</sup> und zudem einmal rechtmäßig erhobene Daten laufend zu wechselnden, vorher nicht festgelegten Zwecken<sup>20</sup> verarbeitet werden. Damit soll gewährleistet werden, dass die betroffene Person den Überblick und die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten nicht verliert.<sup>21</sup>

## II. Der Zweck innerhalb der Rechtsgrundlagen

Auf den ersten Blick wird einem die Bedeutung des Verarbeitungszwecks im Rahmen der Rechtsgrundlagen des Art. 6 Abs. 1 UAbs. 1 DS-GVO nicht vollends klar. So verweist lediglich die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a)

---

Specht/Mantz/Mantz/Marosi, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 88, „Zweckbindung im eigentlichen Sinne“.

<sup>17</sup> Englisch: „*purpose limitation*“, Französisch: „*limitation des finalités*“, Spanisch: „*limitación de la finalidad*“, Italienisch: „*limitazione della finalità*“.

<sup>18</sup> Vgl. zur Kritik an der deutschen Sprachfassung im Vergleich zur englischen Fassung auch Kühling/Buchner/Herbst, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 27, wobei sich die Kritik dort eher darauf bezieht, dass es bereits an einer strengen „Zweckbindung“ fehle.

<sup>19</sup> BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 13; Moos/Schefzig/Arning/Moos, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 4, Rn. 10; Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 13; Spies, ZD 2022, S. 75, 76; Ziegenhorn/Schulz-Große, ZD 2023, S. 581, 583; Leeb/Liebhauer, JuS 2018, S. 534, 537.

<sup>20</sup> Vgl. DatKomm/Hötzendorfer/Tschobl/Kastelitz, Stand: 76. EL. 2023, Art. 5 DS-GVO (Stand: Juli 2020), Rn. 28, „Selbstbindung“; Kühling/Buchner/Herbst, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 22; Schantz, NJW 2016, S. 1841, 1844; siehe auch Spies, ZD 2022, S. 75, 77, wonach „hypothetisch festlegbare“ Zwecke nicht ausreichen.

<sup>21</sup> Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 349; vgl. BeckOK Datenschutzrecht/Schantz, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 18 f.; Culik/Döpke, ZD 2017, S. 226, 227; Freund u.a./Schmidt, DSGVO, 2023, Art. 5 DS-GVO, Rn. 28; siehe auch Kühling/Buchner/Herbst, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 22, für die betroffenen Personen „überschaubar“ und die Aufsichtspersonen „überprüfbar“.



DS-GVO auf den Zweck der Verarbeitung und legt fest, dass betroffene Personen für einen oder mehrere Zwecke ihre Einwilligung in die Datenverarbeitung geben können.<sup>22</sup> In den anderen Rechtsgrundlagen wird nicht ausdrücklich auf den Zweck der Verarbeitung verwiesen. Dennoch liegt der Zweck der Verarbeitung bzw. dessen übergeordnetes Prinzip allen Rechtsgrundlagen zugrunde.<sup>23</sup> Keine der Rechtsgrundlagen macht jedoch Vorgaben hinsichtlich des konkreten Verarbeitungszwecks.

Dies gilt aber auch für die Einwilligung, die zwar in Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO konkret auf den Zweck verweist. Dort heißt es allerdings nur, dass die betroffene Person mindestens für einen Zweck eingewilligt haben muss. Welche (konkreten) Verarbeitungszwecke hiervon umfasst sind, definiert die Datenschutz-Grundverordnung nicht selbst.<sup>24</sup> Es liegt vielmehr an dem Verantwortlichen (und der betroffenen Person)<sup>25</sup>, die konkreten Zwecke der Verarbeitung innerhalb der Einwilligung festzulegen, (vgl. auch ErwG 32 S. 4 DS-GVO).<sup>26</sup>

---

<sup>22</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 10, wonach aus der Rechtsgrundlage der Einwilligung die Anknüpfung an den Zweck „*besonders deutlich wird*“; ähnlich auch BeckOK Datenschutzrecht/*Wolff*, Stand: 46. Ed. 2023, Syst. A. Prinzipien des Datenschutzrechts (Stand: November 2021), Rn. 21.

<sup>23</sup> Vgl. BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 10; BeckOK Datenschutzrecht/*Wolff*, Stand: 46. Ed. 2023, Syst. A. Prinzipien des Datenschutzrechts (Stand: November 2021), Rn. 21; *Dammann*, ZD 2016, S. 307, 311; *Gola/Heckmann/Pöppers*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 14; siehe auch *Gola/Heckmann/Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 18, wonach die Rechtsgrundlagen „*gedanklich um ‚zu einem bestimmten Zweck‘ zu erweitern*“ sind.

<sup>24</sup> Siehe *Veil*, NJW 2018, S. 3337, 3338, der darauf abstellt, dass die Zwecke bei einer Einwilligung „*nicht beschränkt sind*“; siehe auch *Jungkind/Koch*, ZD 2022, S. 656, 658, „*since consent is by law not restricted to certain predefined legitimate purposes*“.

<sup>25</sup> In der Regel dürfte es der Verantwortliche sein, der die Initiative ergreift und eine Einwilligung „*einholt*“ und damit sowohl die Verarbeitung als auch ihren Zweck vorab festlegt. Die betroffene Person wird dann meist nur noch um ihre Zustimmung gebeten. Große Einwirkungsmöglichkeiten der betroffenen Person auf den Inhalt der Einwilligung dürften daher eher selten sein (vgl. hierzu auch Art. 7 Abs. 2 DS-GVO, der gerade auf das „*Ersuchen um Einwilligung*“ abstellt).

<sup>26</sup> *Plath/Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 9; *Gierschmann u.a./Gierschmann*, Datenschutz-Grundverordnung, 2018, Art. 7 DS-GVO, Rn. 73; siehe auch *Däubler u.a./Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 18, Festlegung der Zwecke unter Beachtung des Zweckbindungsgrundsatzes.

Dies lässt sich auch aus der Definition einer wirksamen Einwilligung nach Art. 4 Nr. 11 DS-GVO ableiten. Denn dort wird vorausgesetzt, dass die Einwilligung für den „bestimmten Fall“<sup>27</sup> zu erfolgen hat. Diese Voraussetzung schließt u.a. mit ein, dass der Zweck der Verarbeitung in der Einwilligung festgelegt sein muss, vgl. auch ErwG 42 S. 4 DS-GVO.<sup>28</sup>

Die anderen Rechtsgrundlagen gehen einen etwas anderen Weg. Vergleicht man diese untereinander, so fällt zunächst auf, dass all diese Rechtsgrundlagen eine Art thematische Beschreibung vorgeben. Diese sind:

- vertragliche Interessen (Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO)
- gesetzliche Interessen (Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO)
- lebenswichtige Interessen (Art. 6 Abs. 1 UAbs. 1 lit. d) DS-GVO)
- öffentliche Interessen (Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO)
- berechnigte Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO)

Aufgrund ihrer Abstraktheit<sup>29</sup> dürften diese aber nicht den Anforderungen an den konkreten Zweck einer Verarbeitung gerecht werden, den Art. 5 Abs. 1

<sup>27</sup> Englisch: „specific“, Französisch: „spécifique“, Spanisch: „especifica“, Italienisch: „specifica“, Niederländisch: „specifiek“.

<sup>28</sup> Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 23, der Tatbestand des bestimmten Falls als „Oberbegriff“ für den Zweck der Verarbeitung; BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 78; vgl. Ehmann/Selmayr/Heckmann/Paschke, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 63, ohne auf den konkreten Tatbestand des Art. 4 Nr. 11 DS-GVO abzustellen.

<sup>29</sup> Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 87; Ziegenhorn/Schulz-Große, ZD 2023, S. 581, 583, „abstrakt-generell vorgegebenen Zwecke“; siehe zu den Entwurfsfassungen Richter, DuD 2015, S. 735, 736, „mit extrem breit formulierten Zweckbestimmungen“; Breyer, DuD 2018, S. 311, 313, „grobe Raster“; vgl. auch BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 2, die bei den Rechtsgrundlagen von „rahmenartig gestaltet“ sprechen, dies allerdings nicht explizit auf die Zwecke beziehen; ähnlich Franzen/Gallner/Oetker/Franzen, Eu-ArbRK, 5. Aufl. 2024, 270. Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 2, spricht von „generalklauselartig umschrieben“; auch ähnlich Wybitul/Pöiters/Rauer, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 2 f., „generalklauselartig formuliert“ und „abstrakt und offen formuliert“.

lit. b) DS-GVO hierzu vorsieht.<sup>30</sup> Dennoch steht hinter dieser thematischen Beschreibung dasselbe Prinzip. Denn wenn der Zweck der Verarbeitung den Grund darstellt, warum die personenbezogenen Daten verarbeitet werden sollen, dann stellen diese Themenbereiche einen entsprechenden Rahmen für die konkreten Verarbeitungszwecke dar.<sup>31</sup>

Bspw. stellt die Verarbeitung für die Erfüllung eines Vertrages, wie sie in Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO genannt ist, keinen konkreten Verarbeitungszweck dar. Beruft sich der Verantwortliche allgemein auf ein vertragliches Interesse, reicht dies nicht aus, um eine Datenverarbeitung zu diesem „Zweck“ auf ihre Rechtmäßigkeit hin zu prüfen, da der Zweck der Verarbeitung nicht den Anforderungen nach Art. 5 Abs. 1 lit. b) DS-GVO genügt. Hat der Verantwortliche hingegen einen Vertrag mit der betroffenen Person über den Kauf einer Ware und deren Versand an die betroffene Person geschlossen und möchte nun die Adressdaten der betroffenen Person zum Versand der Warenbestellung verarbeiten, so würde dies für einen konkreten Verarbeitungszweck erfolgen.<sup>32</sup>

---

<sup>30</sup> Simitis/Hornung/Spiecker gen. Döhmman/*Rofßnagel*, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 87; *Breyer*, DuD 2018, S. 311, 313; vgl. auch die Differenzierung bei Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 149 speziell zur Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; vgl. Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 402, wonach der Zweck „innerhalb des Rechtsgrunds“ liegen muss; ähnlich *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 583. Siehe auch zu den Entwurfsfassungen *Richter*, DuD 2015, S. 735, 736 f., dass hierin keine „‘eindeutige[n]‘ Zwecke“ liegen und diese Aufgabe in Zukunft dem Verantwortlichen und in Überprüfung den Gerichten zufällt.

<sup>31</sup> Vgl. in diesem Sinne wohl auch Simitis/Hornung/Spiecker gen. Döhmman/*Rofßnagel*, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 87; Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 402, wonach der Zweck eben „innerhalb des Rechtsgrunds“ liegen muss; ähnlich *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 583. Siehe auch Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 149, mit ihrer Differenzierung zwischen Zweck und berechtigtem Interesse am Beispiel des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; siehe in diese Richtung auch Artikel-29-Gruppe, WP 217, S. 24; mit einer ähnlichen Differenzierung *Herfurth*, ZD 2018, S. 514, 514.

<sup>32</sup> Zu diesem Beispiel im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO allgemein: *Kühling/Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 39, dort speziell zur Frage der Erforderlichkeit; auch *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 382; ebenfalls Simitis/Hornung/Spiecker gen. Döhmman/*Schantz*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 34; *Knyrim/Haidinger*, Praxishandbuch Da-

Die Verarbeitung von Adressdaten für den Warenversand stellt ferner ein vertragliches Interesse i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO dar. Damit fällt der konkrete Zweck in den Themenbereich der Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO. Die Verarbeitung könnte somit, sofern die weiteren Voraussetzungen erfüllt sind, auf diese Rechtsgrundlage gestützt werden.

Um einen breiteren Anwendungsbereich in den Art. 6 Abs. 1 UAbs. 1 lit. b) bis f) DS-GVO zu gewährleisten, geben diese Rechtsgrundlagen daher keinen konkreten Zweck einer Verarbeitung vor.<sup>33</sup> Sie können damit auch nicht die Anforderungen an den Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b) DS-GVO erfüllen. Stattdessen grenzen sie ihren Anwendungsbereich thematisch ein und schaffen so einen Rahmen, mit dem sich mehrere (thematisch ähnliche) Zwecke erfassen lassen, weshalb man zur Abgrenzung auch von einem „Zweckrahmen“ sprechen könnte, der diesen Rechtsgrundlagen zugrunde liegt.<sup>34</sup>

---

tenschutzrecht, 4. Aufl. 2020, Rn. 5.65; *Leeb/Liebhaber*, JuS 2018, S. 534, 536; Schuster/Grütz-macher/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 29.

<sup>33</sup> Simitis/Hornung/Spiecker gen. *Döhmman/Roßnagel*, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 87.

<sup>34</sup> Siehe in die Richtung einer solchen Abgrenzung: Simitis/Hornung/Spiecker gen. *Döhmman/Roßnagel*, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 87; *Schantz/Wolff/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 402, wonach der Zweck „innerhalb des Rechtsgrunds“ liegen muss; ähnlich *Ziegenhorn/Schulz-Große*, ZD 2023, S. 581, 583; *Schwartmann u.a./Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 149, mit ihrer Differenzierung anhand von Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; ähnlich Artikel-29-Gruppe, WP 217, S. 24. So wohl auch zu der hier vertretenen Differenzierung *BeckOK Datenschutzrecht/Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), einmal mit dem Verweis in Rn. 2, wonach die Rechtsgrundlagen „rahmenartig gestaltet“ sind und später in Rn. 57 die Differenzierung zwischen einer Aufgabe (dort auch mal als „Aufgabenrahmen“ bezeichnet) i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO und dem Zweck der Verarbeitung. Siehe ferner *Spies*, ZD 2022, S. 75 ff., der zwischen der Zweckfestlegung durch den Verantwortlichen und dem Gesetzgeber differenziert und dem Gesetzgeber mit der Anforderung einer „hinreichenden Bestimmtheit“ gegenüber dem „konkreten Zweck“ wohl einen Spielraum lässt (vgl. S. 80), was in eine ähnliche Richtung wie die hier vertretene Differenzierung zwischen „Zweck“ und „Zweckrahmen“ verstanden werden könnte.

### *III. Zwischenergebnis*

Festhalten lässt sich, dass alle Rechtsgrundlagen nach Art. 6 Abs. 1 DS-GVO grundlegend am Zweck der Verarbeitung ausgerichtet sind. Die Rechtsgrundlagen schreiben jedoch selbst keinen konkreten Zweck für eine Verarbeitung in ihrem Anwendungsbereich vor. Das System unterscheidet hier zwischen der Einwilligung nach Art. 6 Abs. 1 lit. a) DS-GVO und den übrigen Rechtsgrundlagen.

Die Einwilligung verlangt, dass der Zweck oder die Zwecke der Verarbeitung innerhalb der Einwilligung festgelegt wurden. Welche Zwecke dies umfasst, bestimmt sich i.d.R. nach der Festlegung des Verantwortlichen in dem Einwilligungsersuchen und vor allem nach der Zustimmung der betroffenen Person zu diesem/n Zweck/en.

Die anderen Rechtsgrundlagen hingegen geben einen thematischen Bereich vor. Dieser fungiert als Zweckrahmen für mehrere, thematisch ähnliche Zwecke, die sich jeweils darunter fassen lassen.

## C. Der Legitimationsgedanke hinter den Rechtsgrundlagen

Wie dargestellt wurde, sind alle Rechtsgrundlagen an dem Zweck der Verarbeitung ausgerichtet. Doch was zeichnet die Rechtsgrundlagen als solche aus bzw. woher nehmen die sechs Rechtsgrundlagen nach Art. 6 Abs. 1 DS-GVO ihre Legitimation, über die Rechtmäßigkeit einer Datenverarbeitung zu entscheiden? Für ein besseres Verständnis über das System der Rechtsgrundlagen und ihrer Funktionsweise ist diese Frage von entscheidender Bedeutung.

### *I. Die Aufteilung in Einwilligung und gesetzliche Rechtsgrundlagen*

In seiner Gesamtheit verfolgt Art. 6 Abs. 1 DS-GVO zwei verschiedene Legitimationsgedanken. Ausgehend hiervon lassen sich die Rechtsgrundlagen daher grob in zwei Gruppen aufteilen. Die erste Gruppe umfasst die Einwilligung

nach Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO. Man spricht hier auch von der „*gewillkürten Erlaubnis*“<sup>35</sup> (bzw. hier „Rechtsgrundlage“). Die zweite Gruppe umfasst die übrigen Rechtsgrundlagen. Bei diesen spricht man auch von „*gesetzlichen Erlaubnistatbeständen*“<sup>36</sup> (hier dann „gesetzlichen Rechtsgrundlagen“).

Wie oben dargestellt, verfolgen alle gesetzlichen Rechtsgrundlagen das Prinzip des vorgegebenen Zweckrahmens, während die Einwilligung hier einen Sonderweg beschreitet. Es ist kein Zufall, dass die Gruppen bei der systematischen Unterscheidung der Rechtsgrundlagen hinsichtlich ihres Zwecks bzw. Zweckrahmens mit der hier vorgenommenen Einteilung in Einwilligung und gesetzliche Rechtsgrundlagen übereinstimmen. Beides lässt sich auf den Legitimationsgedanken der Rechtsgrundlagen zurückführen.

Die unterschiedlichen Legitimationsgedanken hängen allgemein mit dem Erfordernis einer Rechtsgrundlage zusammen. Wie bereits gesagt, verlangt das europäische Datenschutzrecht eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, um die Gefahren, die sich aus einer Verarbeitung für die Rechte der betroffenen Personen ergeben können, zu reduzieren. Dabei ist das Erfordernis einer Rechtsgrundlage gleichzeitig Ausdruck des dahinterstehenden Grundrechtsschutz.<sup>37</sup> Nach Art. 8 GrCh<sup>38</sup> ist der Schutz personenbezogener

<sup>35</sup> Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 1; vgl. Dat-Komm/Kastelitz/Hötzendorfer/Tschohl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 20, „*gewillkürter Zulässigkeitstatbestand*“; Chibanguza/Kuß/Steeger/Steeger/Kuß, Künstliche Intelligenz, 2022, § 2, C., Rn. 32, „*gewillkürte Form der Zulässigkeit*“.

<sup>36</sup> Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 1a; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 10; Plath/Plath/Struck, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 4; vgl. auch Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 1, „*gesetzliche Erlaubnis*“.

<sup>37</sup> Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 7; Simitis/Hornung/Spiecker gen. Döhmann/Albrecht, Datenschutzrecht, 2019, Einf. Art. 6 DS-GVO, Rn. 1 f.; vgl. Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 1.

<sup>38</sup> Der EuGH zieht ergänzend noch den allgemeinen Schutz der Privatheit nach Art. 7 GrCh heran, wenn es um den Schutz personenbezogener Daten geht: EuGH, verb. Rs. C-92/09, C-93/09 (Volker und Markus Schecke und Eifert), ECLI:EU:C:2010:662 = EuZW 2010, S. 939, Rn. 47, 52; EuGH, verb. Rs. C-293/12, C-594/12 (Digital Rights Ireland und Seitlinger u.a.), ECLI:EU:C:2014:238 = EuZW 2014, S. 459, Rn. 29 f., 53; EuGH, Rs. C-311/18 (Facebook Ireland und Schrems), ECLI:EU:C:2020:559 = GRUR-RS 2020, 16082, insb. Rn. 168 ff., zudem prüft der EuGH in den anderen Fragen beide Artikel gemeinsam; Streinz/Streinz,

Daten grundrechtlich abgesichert.<sup>39</sup> Ein Eingriff, in Form einer Verarbeitung dieser Daten,<sup>40</sup> bedarf daher der „Rechtfertigung“<sup>41, 42</sup>.

Die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 DS-GVO setzen an diesem Punkt an und stellen auf einfachgesetzlicher Ebene die Rahmenbedingun-

---

EUV/AEUV, 3. Aufl. 2018, Art. 8 GrCh, Rn. 7, der jedoch vom Vorrang des Art. 8 zu Art. 7 GrCh ausgeht; so auch *Jarass*, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 GrCh, Rn. 4. Eine klare Abgrenzung zwischen beiden Grundrechten nimmt der EuGH dabei aber nicht vor: *Kübling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 50, mit kritischer Anmerkung zur fehlenden Abgrenzung der beiden Grundrechte; ebenfalls kritisch: Heselhaus/Nowak/Breuer, Hdb. der Europäischen Grundrechte, 2. Aufl. 2020, § 25, Rn. 20 ff.; *Guckelberger*, EuZW 2011, S. 126, 127; siehe auch zum Verhältnis der beiden Grundrechte *Michl*, DuD 2017, S. 349 ff.; *Rofsnagel*, NJW 2019, S. 1, 2.

<sup>39</sup> EuGH, Rs. C-291/12 (Schwarz), ECLI:EU:C:2013:670 = ZD 2013, S. 608, Rn. 24; EuGH, Rs. C-70/18 (A u.a.), ECLI:EU:C:2019:823 = BeckRS 2019, 23122, Rn. 53; EuGH, Rs. C-311/18 (Facebook Ireland und Schrems), ECLI:EU:C:2020:559 = GRUR-RS 2020, 16082, Rn. 169; *Calliess/Ruffert/Kingreen*, EUV/AEUV, 6. Aufl. 2022, Art. 8 GrCh, Rn. 10; *Meyer/Hölscheidt/Bernsdorff*, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019, Art. 8 GrCh, Rn. 1, 20 ff.; *Schwarze/Knecht*, EU-Kommentar, 4. Aufl. 2019, Art. 8 GrCh, Rn. 4 f.

<sup>40</sup> *Calliess/Ruffert/Kingreen*, EUV/AEUV, 6. Aufl. 2022, Art. 8 GrCh, Rn. 13; *Frenz*, Hdb. Europarecht, 4. Bd. Europäische Grundrechte, 2009, Rn. 1404; *Schwarze/Knecht*, EU-Kommentar, 4. Aufl. 2019, Art. 8 GrCh, Rn. 6; *Specht/Mantz/Bretthauer*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 2, Rn. 16 f.; *Kübling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 52; *Rofsnagel*, NJW 2019, S. 1, 2; vgl. Heselhaus/Nowak/Breuer, Hdb. der Europäischen Grundrechte, 2. Aufl. 2020, § 25, Rn. 47.

<sup>41</sup> Im Zusammenhang der Einwilligung gibt es die Diskussion, ob es sich bei der Einwilligung um eine Rechtfertigung des Grundrechtseingriffs handelt oder ob die Einwilligung bereits den Grundrechtseingriff entfallen lässt. Zur Einordnung als Eingriffsausschluss: *Jarass*, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 GrCh, Rn. 10; *Calliess/Ruffert/Kingreen*, EUV/AEUV, 6. Aufl. 2022, Art. 8 GrCh, Rn. 14; von der Groeben/Schwarze/Hatje/Augsberg, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 8 GrCh, Rn. 12; *Frenz*, Hdb. Europarecht, 4. Bd. Europäische Grundrechte, 2009, Rn. 1417. Eine Entscheidung in dieser Frage ist hier jedoch nicht von Belang.

<sup>42</sup> *Kübling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 53; *Calliess/Ruffert/Kingreen*, EUV/AEUV, 6. Aufl. 2022, Art. 8 GrCh, Rn. 15 ff.; *Specht/Mantz/Bretthauer*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 2, Rn. 20 ff.; *Frenz*, Hdb. Europarecht, 4. Bd. Europäische Grundrechte, 2009, Rn. 1426 ff.

gen für diese Rechtfertigung dar und dienen daher dazu, den Grundrechtsschutz einfachgesetzlich zu verwirklichen.<sup>43</sup> Zur Rechtfertigung kennt Art. 8 Abs. 2 GrCh dabei die Einwilligung der betroffenen Person und sonstige, gesetzlich legitime Grundlagen. Art. 6 Abs. 1 UAbs. 1 DS-GVO spiegelt diese Vorgaben einfachgesetzlich wider, indem die Vorschrift neben der Einwilligung die Fälle der legitimen gesetzlichen Grundlagen ausfüllt.<sup>44</sup>

Auch wenn Art. 6 Abs. 1 DS-GVO damit ein konkretisiertes Abbild des dahinterstehenden Grundrechtsschutzes darstellt, ist außer der grundrechtlichen Vorgaben noch nicht ersichtlich, woher die Einwilligung und die gesetzlichen Rechtsgrundlagen ihre Legitimation für die Rechtfertigung eines Eingriffs in die datenschutzrechtlichen Interessen der betroffenen Personen nehmen.

## II. Die Selbstbestimmung der betroffenen Person als Legitimation

Wenige Probleme bereitet der Legitimationsgedanke hinter der Einwilligung. Aus den vorherigen Ausführungen lässt sich bereits die Legitimation der Einwilligung als Rechtsgrundlage ableiten und spätestens nach einem Blick auf ihre Definition gem. Art. 4 Nr. 11 DS-GVO dürfte schnell klar werden, warum die Einwilligung sowohl in Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO als auch schon in Art. 8 Abs. 2 GrCh – obwohl die Definition der Datenschutz-Grundverordnung als niederrangiges Sekundärrecht für die Auslegung des Primärrechts

---

<sup>43</sup> Simitis/Hornung/Spiecker gen. Döhmann/*Albrecht*, Datenschutzrecht, 2019, Einf. Art. 6 DS-GVO, Rn. 1 f.; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 7 f.; Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 1; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 10.

<sup>44</sup> Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 4; *Veil*, NJW 2018, S. 3337, 3338.



grds.<sup>45</sup> nicht gilt –<sup>46</sup> eine Verarbeitung personenbezogener Daten legitimieren kann. Grundlegend beschreibt die Einwilligung die Zustimmung der betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten.<sup>47</sup> Die betroffene Person stimmt mit ihrer Einwilligung damit auch dem Eingriff in ihre

---

<sup>45</sup> Allgemein zur Auslegung des Primärrechts durch das Sekundärrecht: EuGH, Rs. C-36/74 (Walrave und Koch/Association Union Cycliste Internationale u.a.), ECLI:EU:C:1974:140 = BeckRS 2004, 70975, Rn. 16/19 ff.; EuGH, Rs. C-48/75 (Royer), ECLI:EU:C:1976:57 = BeckRS 2004, 73177, Rn. 10/11 ff.; EuGH, Rs. C-13/78 (Eggers), ECLI:EU:C:1978:182 = BeckRS 2004, 71501, Rn. 23; *Rotb*, *RabelsZ* 75 (2011), S. 787, 812 ff.; *Grundmann*, *RabelsZ* 75 (2011), S. 882, 909 ff.; siehe auch Jung/*Krebs/Stiegler/Krebs/Jung*, *Gesellschaftsrecht in Europa*, 2019, § 2 Europäische Rechtsmethodik, Rn. 134, die einer Auslegung des Primärrechts durch das Sekundärrecht aufgrund des Primärrechtsvorrangs kritisch gegenüberstehen und schlagen daher eine Berücksichtigung des Sekundärrechts mittels einer Begründungslast vor; ablehnend zur Auslegung des Primärrechts durch das Sekundärrecht *Anweiler*, *Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften*, 1997, S. 195 ff. (siehe zur Kritik, S. 197 f.).

<sup>46</sup> Allerdings wird im Zusammenhang des Art. 8 GrCh stellenweise auf das Sekundärrecht verwiesen: *Calliess/Ruffert/Kingreen*, *EUV/AEUUV*, 6. Aufl. 2022, Art. 8 GrCh, Rn. 14, mit Verweis auf die Datenschutz-Grundverordnung; *Meyer/Hölscheidt/Bernsdorff*, *Charta der Grundrechte der Europäischen Union*, 5. Aufl. 2019, Art. 8 GrCh, Rn. 28 f., mit Verweis auf die Datenschutzrichtlinie von 1995; siehe auch mit Verweisen auf die frühere Datenschutzrichtlinie *Heselhaus/Nowak/Breuer*, *Hdb. der Europäischen Grundrechte*, 2. Aufl. 2020, § 25, deren Gehalt für die Auslegung des Art. 8 GrCh allerdings wohl zurückhaltender ansieht (Rn. 47, „in Anlehnung an die Datenschutz-RL“). Der Verweis auf die Datenschutz-Richtlinie (und die Datenschutz-Grundverordnung als Nachfolgerin) könnte mit der Erklärung zu Art. 8 GrCh begründet werden, in der darauf hingewiesen wird, dass Art. 8 GrCh sich u.a. auf die damalige Richtlinie stützt (vgl. Erläuterungen zur Charta der Grundrechte, *ABl. EU C* 303, vom 14.12.2007, S. 17, 20), siehe auch zur Bedeutung u.a. des Sekundärrechts für die Auslegung des Art. 8 GrCh *Calliess/Ruffert/Kingreen*, *EUV/AEUUV*, 6. Aufl. 2022, Art. 8 GrCh, Rn. 8.

<sup>47</sup> *Kuner/Bygrave/Docksey/Kotschy*, *GDPR*, 2020, p. 329; *BeckOK Datenschutzrecht/Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 29; *Schwartzmann u.a./Jacquemain u.a.*, *DS-GVO/BDSG*, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 11; *Auernhammer/Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 17; *Taeger/Gabel/Taeger*, *DSGVO – BDSG – TTDSG*, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 27.

Rechte zu.<sup>48</sup> Sie ist somit Ausdruck der Selbstbestimmung der betroffenen Person im Umgang mit ihren Daten.<sup>49</sup>

Aus dem Selbstbestimmungscharakter lässt sich nun zudem ableiten, warum die Datenschutz-Grundverordnung keine inhaltlichen Vorgaben hinsichtlich der Verarbeitungszwecke macht, wie es bei den gesetzlichen Rechtsgrundlagen durch die Definition eines Zweckrahmens der Fall ist.<sup>50</sup> Die Definition eines Zweckrahmens oder andere inhaltliche Vorgaben an den Verarbeitungszweck im Rahmen der Einwilligung durch den Gesetzgeber käme einer Einschränkung gleich, die mit dem Legitimationsgedanken der Einwilligung grds.<sup>51</sup> nicht vereinbar wäre. Denn der Gesetzgeber könnte damit entscheiden, in welche Verarbeitungen die betroffene Person einwilligen kann und in welche nicht. Dies käme einer gesetzlichen Fremdbestimmung gleich. Eine Einwilligung soll aber gerade der selbstbestimmende Ausdruck der betroffenen Person und damit frei von *jeglicher* Fremdbestimmung sein.<sup>52</sup> Ziel des Datenschutzrechts ist der

---

<sup>48</sup> Franzen/Gallner/Oetker/Franzen, EuArbRK, 5. Aufl. 2024, 270. Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 4; Chibanguza/Kuß/Steeger/Steeger/Kuß, Künstliche Intelligenz, 2022, § 2, C., Rn. 32; vgl. Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 27, „Grundrechtsausübung“; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 17, „privatautonome Gestaltung des eigenen Grundrechtsschutzes“.

<sup>49</sup> Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 21; Kühling/Buchner/ Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 17; Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 3; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 17; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 4; vgl. Franzen, EuZA 2017, S. 313, 321. Siehe auch Tinnefeld/Conrad, ZD 2018, S. 391 ff.

<sup>50</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen.*

<sup>51</sup> Die Datenschutz-Grundverordnung kennt hiervon eine Ausnahme. Nach Art. 9 Abs. 2 lit. a) DS-GVO kann das Unionsrecht oder das Recht der Mitgliedstaaten Bereiche vorsehen, in denen betroffene Personen eine Verarbeitung besonderer Kategorien personenbezogener Daten nicht durch eine Einwilligung legitimieren können. Vgl. hierzu auch BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 9 DS-GVO (Stand: August 2023), Rn. 62, wonach aber bei Ausübung dieser Befugnis dem Grundgedanken der Einwilligung Rechnung getragen werden muss; ähnlich Ehmman/Selmayr/Schiff, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 9 DS-GVO, Rn. 36; ebenso Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 9 DS-GVO, Rn. 22 f.

<sup>52</sup> Taeger/Gabel/Arning/Rothkegel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 291, „frei von Paternalismus und Zwang“; vgl. Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 5, der eine Anlehnung an

Schutz der betroffenen Person vor den Gefahren einer Verarbeitung ihrer personenbezogenen Daten (vgl. Art. 1 DS-GVO). Die betroffene Person soll aber nicht (umfassend) vor sich selbst und ihrer eigenen Entscheidung geschützt werden.<sup>53</sup>

Betrachtet man sich in diesem Lichte die Voraussetzungen an eine wirksame Einwilligung, so fällt auch direkt auf, dass diese lediglich darauf abzielen, den Selbstbestimmungscharakter zu wahren.<sup>54</sup> Die Einwilligung muss nach Art. 4 Nr. 11 DS-GVO für den „bestimmten Fall“<sup>55</sup> und in „informierter Weise“<sup>56</sup> abgegeben werden. Die Einwilligung muss also derart bestimmt definiert werden, damit die betroffene Person überhaupt in der Lage ist, den Inhalt und die Reichweite der Datenverarbeitung zu erfassen.<sup>57</sup> Das bedeutet, dass der Zweck der Verarbeitung vorab klar definiert sein muss.<sup>58</sup> An das Bestimmtheitsgebot

---

das Zivilrecht sieht, um Bedingungen zu schaffen, die eine „privatautonome Entscheidung“ gewährleisten können; siehe hierzu auch Simitis/Hornung/Spiecker gen. Döhmman/*Albrecht*, Datenschutzrecht, 2019, Einführung zu Art. 6 DS-GVO, Rn. 4, mit dem Verweis auf das Ziel des Gesetzgebers diese Selbstbestimmung (wieder) zu gewährleisten.

<sup>53</sup> Gierschmann u.a./*Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 48 f.; siehe auch allgemein Taeger/Gabel/*Arning/Rothkegel*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 291, „frei von Paternalismus und Zwang“. Siehe auch *Haase*, InTeR 2019, S. 113 ff., der in Bezug auf den Einwilligungstatbestand der „Freiwilligkeit“ aufzeigt, dass hohe rechtliche Anforderungen hieran gleichfalls zu einer Einschränkung einwilligungsbereiter betroffener Personen und deren Recht auf Schutz ihrer Freiheit zur Selbstbestimmung führen können. Siehe auch Kühling/*Buchner/Buchner/Kühling*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 41, die konkret zum Tatbestand der „Freiwilligkeit“ darauf hinweisen, dass zu enge Anforderungen „die steuernde Kraft einer informationellen Selbstbestimmung in Frage [stellen]“. Allgemeiner mit Fokus auf den datenschutzrechtlichen Grundrechtsschutz *Klement*, JZ 2017, S. 161, 168 f.

<sup>54</sup> *Buchner*, DuD 2016, S. 155, 158, spricht daher bei den Voraussetzungen um „Selbstverständlichkeiten“ mit Hinblick auf ihren „Ausdruck privatautonomer Selbstbestimmung“.

<sup>55</sup> Englisch: „specific“, Französisch: „spécifique“, Spanisch: „especifica“, Italienisch: „specifica“, Niederländisch: „specifiek“.

<sup>56</sup> Englisch: „informed“, Französisch: „éclairée“, Spanisch: „informada“, Italienisch: „informata“, Niederländisch: „geïnformeerde“.

<sup>57</sup> BeckOK Datenschutzrecht/*Stemmer*, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 77; *Ehmann/Selmayr/Heckmann/Paschke*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 63; Simitis/Hornung/Spiecker gen. Döhmman/*Klement*, Datenschutzrecht, 2019, Art. 7 DS-GVO, Rn. 69; *Veil*, NJW 2018, S. 3337, 3340.

<sup>58</sup> Kühling/*Buchner/Buchner/Kühling*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 61 f.; Simitis/Hornung/Spiecker gen. Döhmman/*Klement*, Datenschutzrecht, 2019, Art. 7

knüpft anschließend die Informationspflicht an.<sup>59</sup> Die betroffene Person muss über die festgelegten Modalitäten informiert werden, um auf Basis dieser Informationen die Entscheidung zu treffen.<sup>60</sup> Dies schafft die Ausgangslage, damit die betroffene Person überhaupt selbstbestimmend über die Verarbeitung ihrer Daten entscheiden kann.<sup>61</sup>

Darüber hinaus muss die Zustimmung „freiwillig“<sup>62</sup> erfolgen.<sup>63</sup> Dies soll konkret verhindern, dass fremdbestimmende Faktoren die Zustimmung der betroffenen Person beeinflussen und die Einwilligung somit ihren selbstbestimmenden Charakter verliert, der ihrem Legitimationsgedanken zugrunde liegt.<sup>64</sup>

---

DS-GVO, Rn. 70; Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 39; BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 78; Moos/Schefzig/Arning/Rohwedder, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 270; Veil, NJW 2018, S. 3337, 3340.

<sup>59</sup> Krohm, ZD 2016, S. 368, 373; vgl. Simitis/Hornung/Spiecker gen. Döhmman/Klement, Datenschutzrecht, 2019, Art. 7 DS-GVO, Rn. 72, „subjektive Gegenstück zur Bestimmtheit“; Kühling/Buchner/Buchner/Kühling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 63, die Bestimmtheit als „notwendige Voraussetzung“ der Informiertheit; vgl. auch Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, 518; siehe auch BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 78; Thüsing/Thüsing/Traut, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 5, Rn. 14, mit Verweis auf einen „engen Zusammenhang“ beider Voraussetzungen.

<sup>60</sup> Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 34; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 37 f.; Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 517; Kollmar/El-Auwad, K&R 2021, S. 73, 75.

<sup>61</sup> Vgl. BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 55; Knyrim/Wyrobek, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 6.30; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 37; Franzen, EuZA 2017, S. 313, 322, als „unabdingbare Voraussetzung für eine freiwillige Entscheidung“; ähnlich Kollmar/El-Auwad, K&R 2021, S. 73, 75; siehe auch Chibanguza/Kuß/Steege/Steege/Kuß, Künstliche Intelligenz, 2022, § 2, C., Rn. 34.

<sup>62</sup> Englisch: „freely given“, Französisch: „libre“, Spanisch: „libre“, Italienisch: „libera“, Niederländisch: „vrij“.

<sup>63</sup> BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 39 ff.; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 7 DS-GVO, Rn. 88 ff.; Kühling/Buchner/Buchner/Kühling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 41 ff.; Moos/Schefzig/Arning/Rohwedder, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 257 ff.

<sup>64</sup> Siehe BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 39, als Bedeutung für den „Ausdruck individueller Selbstbestimmung“;

Abschließend muss die Zustimmung der betroffenen Person auch „*unmissverständlich*“<sup>65</sup> erfolgen.<sup>66</sup> Bei dieser Voraussetzung handelt es sich mehr um die Sicherstellung, dass die betroffene Person tatsächlich zugestimmt hat.<sup>67</sup>

### III. Die gesetzlichen Rechtsgrundlagen als vordefinierte Eingriffsrechtfertigung

#### 1. Die gesetzlichen Rechtsgrundlagen als Ausdruck einer Grundrechtsabwägung

Anders verhält es sich bei den gesetzlichen Rechtsgrundlagen. Die rechtmäßige Verarbeitung setzt hier nicht die Zustimmung der betroffenen Person voraus.<sup>68</sup>

---

vgl. Simitis/Hornung/Spiecker gen. Döhmman/Klement, Datenschutzrecht, 2019, Art. 7 DS-GVO, Rn. 48; siehe auch Kühling/Buchner/Buchner/Kühling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 41.

<sup>65</sup> Englisch: „*unambiguous*“, Französisch: „*univoque*“, Spanisch: „*inequívoca*“, Italienisch: „*inequivocabile*“, Niederländisch: „*ondubbelzinnige*“.

<sup>66</sup> BeckOK Datenschutzrecht/Stemmer, Stand: 46. Ed. 2023, Art. 7 DS-GVO (Stand: November 2023), Rn. 82; DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 26 f.; Taeger/Gabel/Arning/Rothkegel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO, Rn. 349.

<sup>67</sup> Vgl. DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 26; Taeger/Schweda, ZD 2020, S. 124, 125; Thüsing/Thüsing/Traut, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 5, Rn. 24; siehe auch Knyrim/Wyrobek, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 6.37, „*bewusste Entscheidung der betroffenen Person*“, aber nicht mit direktem Bezug zum Tatbestand der Unmissverständlichkeit.

<sup>68</sup> Differenzierter ließe sich dies bei der Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO betrachten, denn die Verarbeitung aufgrund vertraglicher Interessen stützt sich auf dem Willen der betroffenen Person an diesem Vertrag. Vgl. hierzu: Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 5; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 26; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 21; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 60; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 27; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 41; Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 38; Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 15; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 29; Klein, Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?, in: FS Taeger, 2020, S. 235, 245; Heinzke/Engel, ZD 2020, S. 189, 189.

Auf Basis der gesetzlichen Rechtsgrundlagen können sogar Verarbeitungen personenbezogener Daten vorgenommen werden, die ausdrücklich dem Willen der betroffenen Person entgegenstehen.<sup>69</sup> Die Legitimation leitet sich damit nicht aus dem Willen der betroffenen Person ab, sondern hat ihren Ursprung in den dahinterstehenden Grundrechten einerseits und den schutzwürdigen Interessen des Verantwortlichen andererseits. Wie bereits erwähnt, ist der Schutz personenbezogener Daten in Art. 8 GrCh grundrechtlich abgesichert. Das Grundrecht nach Art. 8 GrCh gilt jedoch nicht absolut.<sup>70</sup> Im Falle der gesetzlichen Rechtsgrundlagen ist zu bedenken, dass nicht nur der Schutz personenbezogener Daten grundrechtlich gesichert ist. Das Interesse an einer Datenverarbeitung kann ebenfalls Grundrechtsschutz genießen (bspw. durch die Berufsfreiheit oder die Meinungsfreiheit, vgl. auch ErwG 4 DS-GVO).<sup>71</sup>

Allgemein gibt es daher auch geschützte Interessen an der Verarbeitung personenbezogener Daten. Die gesetzlichen Rechtsgrundlagen greifen diesen Gedanken auf und verkörpern auf einfachgesetzlicher Ebene das Ergebnis der Abwägung zwischen dem Interesse am Schutz vor einer Datenverarbeitung und dem Interesse an der Verarbeitung.<sup>72</sup> Es handelt sich bei ihnen daher um Fälle,

<sup>69</sup> Vgl. auch *Sundermann*, DuD 2021, S. 594, 596, der die gesetzlichen Rechtsgrundlagen als Einschränkung der „*Dispositionsfähigkeit der betroffenen Person*“ einordnet.

<sup>70</sup> EuGH, verb. Rs. C-92/09, C-93/09 (Volker und Markus Schecke und Eifert), ECLI:EU:C:2010:662 = EuZW 2010, S. 939, Rn. 48; EuGH, Urteil v. 16.07.2020, Rs. C-311/18 (Facebook Ireland und Schrems), ECLI:EU:C:2020:559 = GRUR-RS 2020, 16082, Rn. 172; EuGH, Rs. C-439/19 (Latvijas Republikas Saeima ([Points de pénalité])), ECLI:EU:C:2021:504 = BeckRS 2021, 15289, Rn. 105; Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 4; Meyer/Hölscheidt/*Bernsdorff*, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019, Art. 8 GrCh, Rn. 24; vgl. *Jarass*, Charta der Grundrechte der EU, 4. Aufl. 2021, Art. 8 GrCh, Rn. 13 ff.

<sup>71</sup> Vgl. Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 3 f.; BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 1 DS-GVO (Stand: November 2021), Rn. 7; Taeger/Gabel/*Schmidt*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 1 DS-GVO, Rn. 22; Gierschmann u.a./*Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 18 f.; *Veil*, NJW 2018, S. 3337, 3342; *Krusche*, ZD 2020, S. 232, 233; *Roßnagel*, NJW 2019, S. 1, 3.

<sup>72</sup> Vgl. *Roßnagel/Roßnagel*, Das neue Datenschutzrecht, 2018, § 3, Rn. 50; *Roßnagel*, NJW 2019, S. 1, 5; *Jungkind/Koch*, ZD 2022, S. 656, 658; Spiecker gen. Döhmann u.a./*Sartor*, GDPR, 2023, Art. 6 GDPR, Rn. 53, erfasst noch zusätzlich die Einwilligung, bei der die Interessenab-

bei denen das Interesse an einer Datenverarbeitung dem Schutzinteresse der betroffenen Person vor einer Datenverarbeitung überwiegt.<sup>73</sup> Damit erklärt sich dann auch, warum der Gesetzgeber u.a. die Anwendungsbereiche der gesetzlichen Rechtsgrundlagen mit der Definition eines Zweckrahmens eingrenzt. Sie sollen sicherstellen, dass Datenverarbeitungen nur in dem zulässigen Rahmen legitimiert werden. Die gesetzlichen Rechtsgrundlagen sind somit vom Gesetzgeber vordefinierte gerechtfertigte Eingriffe in die Schutzinteressen der betroffenen Personen.<sup>74</sup>

## 2. Verwirklichung der Abwägung

Aufgrund der Vielzahl möglicher Interessen, die eine Verarbeitung personenbezogener Daten rechtfertigen können, kann der Gesetzgeber nicht alle denkbaren Fälle in einer eigenen Rechtsgrundlage aufzuführen. Hierzu dient dann auch die bereits angesprochene Definition eines Zweckrahmens anstelle der Vorgabe

---

wägung durch die betroffene Person vorgenommen wird (siehe auch Rn. 20 f.), was im Wesentlichen der oben beschriebenen Selbstbestimmung entspricht (siehe bereits: Kap. 8, C., II. *Die Selbstbestimmung der betroffenen Person als Legitimation.*); siehe Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 8, mit Verweis auf das „*Verbot mit Erlaubnisvorbehalt*“; vgl. auch Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 3 wobei dieser vorrangig auf die Differenzierung zwischen dem privaten und öffentlichen Bereich abstellt; siehe auch Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 18 f., ebenfalls vorrangig für den nicht öffentlichen Bereich und mit Verweis auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO aus dem diese Abwägung deutlich hervorgehe.

<sup>73</sup> Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 3, Rn. 50; Roßnagel, NJW 2019, S. 1, 5; vgl. Jungkind/Koch, ZD 2022, S. 656, 658; Spiecker gen. Döhmann u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 53. Siehe auch Klaas, CCZ 2020, S. 256, 261, der jedenfalls zu Art. 6 Abs. 1 UAbs. 1 lit. b)-e) DS-GVO darauf verweist, dass der Ordnungsgeber dort die „*Interessen als überwiegend qualifiziert*“ hat und in Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO dies dem Rechtsanwender obliegt; ähnlich Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 13.

<sup>74</sup> Vgl. Schantz/Wolff/Schantz, Das neue Datenschutzrecht, 2017, Rn. 474; Roßnagel/Roßnagel, Das neue Datenschutzrecht, 2018, § 3, Rn. 50; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 10, „*gesetzlich angeordnete Zulässigkeit*“.

konkreter Verarbeitungszwecke.<sup>75</sup> Doch zeigen sich zwischen den einzelnen, gesetzlichen Rechtsgrundlagen Unterschiede in der Art und Weise, wie sie die Abwägung auf der Ebene der hinter ihnen stehenden Interessen umsetzen.<sup>76</sup>

Hierzu lassen sich die gesetzlichen Rechtsgrundlagen in drei Untergruppen (vollkommene Rechtsgrundlagen, ergänzungsbedürftige Rechtsgrundlagen und abwägende Rechtsgrundlage) weiter einteilen.<sup>77</sup>

### a) Vollkommene Rechtsgrundlagen

Unter die vollkommenen Rechtsgrundlagen fallen die Rechtsgrundlagen zugunsten vertraglicher Interessen (Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO) und lebenswichtiger Interessen (Art. 6 Abs. 1 UAbs. 1 lit. d) DS-GVO). Es handelt sich hierbei um vollkommene Rechtsgrundlagen, weil sie so, wie sie in der Datenschutz-Grundverordnung formuliert sind i.S.d. Subsumtionsfähigkeit, vollständig sind. Insbesondere wird der jeweilige Zweckrahmen der Rechtsgrundlage vollständig festgelegt.

Datenverarbeitungen, deren Basis eine dieser beiden Rechtsgrundlagen sein soll, lassen sich unmittelbar unter Art. 6 Abs. 1 UAbs. 1 lit. b) oder d) DS-GVO subsumieren.<sup>78</sup> Anhand des jeweiligen Verarbeitungszwecks ist hinsichtlich der Anwendung einer dieser beiden Rechtsgrundlagen direkt zu prüfen, ob es sich um ein solches vertragliches Interesse oder lebenswichtiges Interesse handelt.

<sup>75</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen*.

<sup>76</sup> Siehe zu einer ähnlichen Darstellung des Abwägungsgedankens hinter den verschiedenen Rechtsgrundlagen Specker gen. Döhmann u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 53. Siehe auch *Klaas*, CCZ 2020, S. 256, 261, jedenfalls mit der Differenzierung zwischen Art. 6 Abs. 1 UAbs. 1 lit. b)-e) DS-GVO und lit. f); ähnlich Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 13.

<sup>77</sup> Vgl. auch Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 4, „mehr oder weniger detailliert ausdifferenzierte Erlaubnistatbestände“.

<sup>78</sup> Vgl. Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 5, wonach die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. a), b), d) und f) DS-GVO „in der DSGVO vollständig geregelt“ sind; ähnlich Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 6, wonach die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. a), b), d) und f) DS-GVO als Abgrenzung zu den beiden Verbleibenden keine „gesonderte Rechtsgrundlagen“ benötigen. Siehe zu weiteren Einordnung der Einwilligung (lit. a)) oben: Kap. 8, C., II. *Die Selbstbestimmung der betroffenen Person als Legitimation* und des berechtigten Interesses (lit. f)) nachfolgend: Kap. 8, C., III., 2., c) *Abwägende Rechtsgrundlage*.



Eine weitere Konkretisierung dieser Rechtsgrundlagen bedarf es nicht. Damit hat der europäische Gesetzgeber vertragliche und lebenswichtige Interessen als geschützte Rechtspositionen qualifiziert, die grundsätzlich in der Lage sind, dem Interesse der betroffenen Personen am Schutz ihrer personenbezogenen Daten zu überwiegen.<sup>79</sup>

### *b) Ergänzungsbedürftige Rechtsgrundlagen*

Die Charakteristika einer vollkommenen Rechtsgrundlage lassen sich am besten anhand ihres Gegenstücks, den ergänzungsbedürftigen Rechtsgrundlagen, verdeutlichen. Die ergänzungsbedürftigen Rechtsgrundlagen sind die rechtliche Verpflichtung (Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO) und die Wahrung des öffentlichen Interesses bzw. die Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO). Anders als die vollkommenen Rechtsgrundlagen können Datenverarbeitungen nicht direkt unter diese Rechtsgrundlagen subsumiert werden.<sup>80</sup> Denn die Zweckrahmen dieser Rechtsgrundlagen wurden vom Gesetzgeber noch nicht abschließend festgelegt und bedürfen einer Konkretisierung.

Dieses Konkretisierungserfordernis geht aus Art. 6 Abs. 3 DS-GVO hervor. Denn danach muss eine Rechtsgrundlage für die Verarbeitung auf Basis der „Art. 6 Abs. 1 lit. c) und e) DS-GVO“<sup>81</sup> entweder im EU-Recht oder im Recht der Mitgliedstaaten verankert sein. Die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO müssen daher in Verbindung mit einer weiteren

---

<sup>79</sup> Spiecker gen. Döhmman u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 53, verweist für Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO auf den Willen der betroffenen Person am Vertragsabschluss (siehe zudem Rn. 33), siehe zu diesem Legitimationsgedanken bereits oben Fn. 68.

<sup>80</sup> Siehe auch die Einordnung, dass es sich bei Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO nicht um eigenständige Erlaubnistatbestände bzw. Rechtsgrundlagen handelt: Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 49, 60; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 73, 83, 120; Taeger/Gabel/Taeger, DS-GVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 155; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 55; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 49, 57.

<sup>81</sup> Es handelt sich um den Wortlaut der Datenschutz-Grundverordnung, der an dieser Stelle Art. 6 Abs. 1 DS-GVO nicht präzise zitiert, siehe auch Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 34. Siehe hierzu bereits: Kap. 8, A. Die Notwendigkeit einer Rechtsgrundlage, Fn. 3.

Rechtsgrundlage aus dem EU-Recht oder dem Recht der Mitgliedstaaten gesehen werden.<sup>82</sup> Bei diesen Rechtsgrundlagen kann man daher von „ergänzenden Rechtsgrundlagen“<sup>83</sup> sprechen.

Die Aufgabe der ergänzenden Rechtsgrundlagen besteht darin, die rechtliche Verpflichtung bzw. die Aufgabe im öffentlichen Interesse/die Ausübung öffentlicher Gewalt, die in Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO zugrunde gelegt werden, zu konkretisieren.<sup>84</sup> Die ergänzende Rechtsgrundlage sagt damit bspw. um welche rechtliche Verpflichtung es sich handelt. Die Datenschutz-Grundverordnung schafft mit diesen Rechtsgrundlagen eine Verbindung zu anderen Rechtsbereichen. Durch die ergänzenden Rechtsgrundlagen i.S.d. Art. 6 Abs. 3 DS-GVO sollen daher Datenverarbeitungen, die in anderen Teilen der Rechtsordnung vorgesehen sind, datenschutzrechtliche Geltung verschafft werden.<sup>85</sup>

Es ist somit Aufgabe des Gesetzgebers der ergänzenden Rechtsgrundlage, die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO zu vervoll-

---

<sup>82</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 49, Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO werden danach als „*Einfallstor*“ für diese Vorschriften bezeichnet; so auch Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 83, speziell zu Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO, siehe aber auch den Verweis in Rn. 120 auf diese Ausführungen im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; auch Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 69; Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 52, 71, 79, „*Scharniernorm*“, siehe ebenso die Kommentierung zu Abs. 3, Rn. 14; ebenso als „*Scharniernormen*“ Roßnagel/*Nebel*, Das neue Datenschutzrecht, 2018, § 3, Rn. 98; siehe auch Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 49 ff., 60.

<sup>83</sup> Vgl. Spindler/Schuster/*Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 8, „*konkretisierenden Grundlage*“ zu Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO.

<sup>84</sup> Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 3; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 77, 94 f.; Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 51, 71, 79; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 88, speziell zu lit. e).

<sup>85</sup> Vgl. Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 592, im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO, siehe aber auch Rn. 597; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 35 spricht im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO hier – etwas weit – von einer „*Subsidiarität des Datenschutzrechts*“ gegenüber anderen Rechtspflichten.

ständigen, indem das Verarbeitungsinteresse, das dem Schutzinteresse der betroffenen Person überwiegen muss, weiter zu definieren. Dabei ist der Gesetzgeber der ergänzenden Rechtsgrundlag nicht vollkommen frei, denn die Verordnung stellt in Art. 6 Abs. 3 DS-GVO Anforderungen an die ergänzende Rechtsgrundlage. Dennoch bedeutet dies im Kontext des hier dargelegten Systems, dass die ergänzenden Rechtsgrundlagen einer Konkretisierung des Zweckrahmens dienen und zu dem dahinterstehenden Interessenausgleich beitragen.<sup>86</sup>

### c) Abwägende Rechtsgrundlage

Zu den vollkommenen und ergänzungsbedürftigen Rechtsgrundlagen tritt eine weitere Gruppe, die abwägende Rechtsgrundlage, hinzu. Diese Untergruppe der gesetzlichen Rechtsgrundlagen besteht lediglich aus Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO.<sup>87</sup> Die Differenzierung und die Abgrenzung zu den beiden vorherigen Gruppen lässt sich aus den zusätzlichen Voraussetzungen dieser Rechtsgrundlage ableiten. Im Gesamtvergleich tritt sie dabei zwischen die vollkommenen und ergänzungsbedürftigen Rechtsgrundlagen.

Ähnlich wie die vollkommenen Rechtsgrundlagen und anders als die ergänzungsbedürftigen Rechtsgrundlagen ist Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO dahingehend abschließend formuliert, dass es keines weiteren Rechtsakts, bspw. in Form einer ergänzenden Rechtsgrundlage, bedarf, um eine Datenverarbeitung unter diese Rechtsgrundlage zu subsumieren. Eine direkte Subsumtion der Verarbeitung bzw. dann konkret deren Zweck, ist unter Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO allerdings dennoch nicht möglich. Dies hängt zusammen mit dem vorgegebenen Zweckrahmen der Rechtsgrundlage.

---

<sup>86</sup> Vgl. Spiecker gen. Döhmann u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 53, siehe auch hinsichtlich einer Abwägung aufgrund der Anforderungen nach Art. 6 Abs. 3 DS-GVO, Rn. 84.

<sup>87</sup> Vgl. Herfurth, ZD 2018, S. 514, 514, als „zentrale Abwägungsklausel“ bei der der verfolgte Interessenausgleich, der hinter „[n]abezu allen Vorschriften der DS-GVO“ steht, am deutlichsten ist. Siehe ebenfalls zur Einordnung als zentrale Abwägungsklausel: Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 59; Schulze/Janssen/Kadelbach/Holznaegel/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 26; Chibanguza/Kuß/Steeger/Steeger/Kuß, Künstliche Intelligenz, 2022, § 2, C., Rn. 47; ähnlich BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 63; siehe auch Albrecht/Joitzo, Das neue Datenschutzrecht der EU, 2017, Teil 3, Rn. 51, „zentrale Stellschrauben [...] für einen gerechten Ausgleich zwischen den Interessen der Verbraucher und der Wirtschaft“.

Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO knüpft an das berechtigte Interesse an. Es ist allerdings nicht ausreichend, eine Datenverarbeitung und deren Zweck unter den Zweckrahmen des berechtigten Interesses zu subsumieren. Denn der Begriff des berechtigten Interesses ist sehr weit und kann praktisch alle Arten von Interessen, wie wirtschaftliche, ideelle oder rechtliche Interessen umfassen.<sup>88</sup> Als einzige Einschränkung wird vorgebracht, dass diese Interessen eben „berechtigt“ sein müssen und nicht gegen die Rechtsordnung verstoßen dürfen.<sup>89</sup> Trotz dieser Einschränkung wäre mit Blick auf den dahinterstehenden Grundrechtsschutz vor einer Verarbeitung personenbezogener Daten ein so

---

<sup>88</sup> Herfurth, ZD 2018, S. 514, 514; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 61; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 68; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 14; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 70; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 95; Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 98; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 146a, nennen zusätzlich noch ausdrücklich „tatsächliche“ Interessen; ebenso Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 145; auch Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 129; auch Härting/Gössling/Dimov, ITRB 2017, S. 169, 171; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 28, stellt allgemein auf ein weites Verständnis ab, nennt aber später auch konkret „wirtschaftliche und ideelle Interessen“; auch für ein weites Verständnis Plath/Plath/Struck, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 62; ebenfalls für ein weites Verständnis Robrahn/Bremert, ZD 2018, S. 291, 291 f.

<sup>89</sup> Herfurth, ZD 2018, S. 514, 514; Plath/Plath/Struck, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 62; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 129; Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 145; Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 98; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 70; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 72, 76; Robrahn/Bremert, ZD 2018, S. 291, 291 f.; Härting/Gössling/Dimov, ITRB 2017, S. 169, 171; kritisch hierzu Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 77, der aus Gründen der Harmonisierung hier allenfalls auf „Unionrechtskonformität“ abstellen möchte; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 61 möchte wohl einen Rechtsverstoß bei der Beurteilung eines berechtigten Interesses berücksichtigen, „illegitime“ Interessen aber dann wohl erst in der darauffolgenden Interessenabwägung (vgl. Rn. 62); weitgehender wohl Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 644, der die „Rechtswidrigkeit“ allgemein wohl erst bei der Interessenabwägung berücksichtigen möchte.

umfangreicher Anwendungsbereich problematisch. Es bedarf daher einer weiteren Konkretisierung der zulässigen Interessen.

Mit dem Erfordernis einer weiteren Konkretisierung nähert sich Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO den ergänzungsbedürftigen Rechtsgrundlagen an, doch – wie bereits gesagt – erfolgt die Konkretisierung in Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO nicht mittels einer ergänzenden Rechtsgrundlage. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO sieht ein anderes Instrument für diese Konkretisierung vor, das bereits in der Rechtsgrundlage selbst verankert ist. Die Rechtsgrundlage verlangt eine Interessenabwägung, bei der das jeweilige Interesse an der Verarbeitung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person abzuwägen ist.<sup>90</sup> Die Interessen der betroffenen Person dürfen im Ergebnis dieser Abwägung nicht überwiegen.<sup>91</sup> Durch diese Abwägung wird der sehr weite Bereich des berechtigten Interesses weiter eingeschränkt.

Die Interessenabwägung hat der Verantwortliche selbst durchzuführen.<sup>92</sup> Mit Blick auf den Streit und das Erfordernis eines Ausgleichs der hinter einer

---

<sup>90</sup> *Herfurth*, ZD 2018, S. 514, 515; *Ehmann/Selmayr/Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 25, 28 ff.; *Gola/Heckmann/Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 59, 62 f.; *Plath/Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 53; *Sydow/Marsch/Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 82 ff.; *Schwartmann u.a./Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 135, 152 ff.; *Däubler u.a./Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 92, 101; *Kuner/Bygrave/Docksey/Kotschy*, GDPR, 2020, p. 338; *Moos/Schefzig/Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 77 ff.; *Härting/Gössling/Dimov*, ITRB 2017, S. 169, 171; vgl. EuGH, verb. Rs. C-468/10, C-469/10 (ASNEF), ECLI:EU:C:2011:777 = EuZW 2012, S. 37, Rn. 40, zu Art. 7 lit. f) DS-RL.

<sup>91</sup> *Herfurth*, ZD 2018, S. 514, 514, 520; *Gola/Heckmann/Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 62; *Sydow/Marsch/Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 87; *Taeger/Gabel/Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 146; *Feiler/Forgó*, EU-DSGVO und DSGVO, 2. Aufl. 2022, Art. 6 DS-GVO, Rn. 29; *Jahnel/Jahnel*, DSGVO, 2021, Art. 6 DS-GVO, Rn. 67; *Moos/Schefzig/Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 77; *Robrahn/Bremert*, ZD 2018, S. 291, 293; *Härting/Gössling/Dimov*, ITRB 2017, S. 169, 170.

<sup>92</sup> *Spindler/Schuster/Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 18; *Ehmann/Selmayr/Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 30, 32; *Paal/Pauly/Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 31; *Plath/Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 58; *Taeger/Gabel/Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-

Verarbeitung stehenden Interessen, delegiert der Gesetzgeber das Problem weiter an den Verantwortlichen.<sup>93</sup> Bevor der Verantwortliche eine Verarbeitung auf Basis des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO vornehmen kann, muss er – und gerade nicht der Gesetzgeber – ermitteln, ob sein Interesse an der Verarbeitung den Schutzinteressen der betroffenen Person überwiegt. Dem Verantwortlichen die Aufgabe der Interessenabwägung zu übertragen, wird durchaus kritisch betrachtet,<sup>94</sup> zumal die Verordnung nur sehr wenige Hinweise enthält, welche Kriterien bei dieser Abwägung zu berücksichtigen sind.<sup>95</sup>

---

GVO, Rn. 119, 142; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 92; Jahnel/Jahnel, DSGVO, 2021, Art. 6 DS-GVO, Rn. 68; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 67; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 87; Spiecker gen. Döhmann u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 54 f.; Simitis/Hornung/Spiecker gen. Döhmann/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 87; siehe bereits zu Art. 7 DS-RL Ferretti, CML Rev. 51 (2014), p. 843, 844 f., 859, mit Blick auf den damaligen Verordnungsvorschlag.

<sup>93</sup> Spiecker gen. Döhmann u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 54; vgl. Klaas, CCZ 2020, S. 256, 261, der darauf verweist, dass bei den anderen gesetzlichen Rechtsgrundlagen die „Abwägung [der Interessen vom Gesetzgeber] vorweggenommen“ wurden; ähnlich Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 13; siehe auch Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 144; die auf die Rechtslage unter der Datenschutzrichtlinie verweisen, wo es ebenfalls das berechnete Interesse als Rechtsgrundlage gab, der Gesetzgeber die Abwägung aber häufig in einzelnen Rechtsvorschriften näher konkretisiert hat.

<sup>94</sup> Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 67 wonach sich der Verantwortliche in einem Interessenkonflikt befindet; ähnlich auch Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 27, der von einem „(Bias)“ des Verantwortlichen spricht; siehe bereits zu Art. 7 DS-RL Ferretti, CML Rev. 51 (2014), p. 843, 861, mit Blick auf den damaligen Verordnungsvorschlag (vgl. auch S. 859).

<sup>95</sup> BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 13; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 14; Simitis/Hornung/Spiecker gen. Döhmann/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 103; Schwartmann u.a./Jacquematn u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 136; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 12; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 82; Buchner, DuD 2016, S. 155, 159; Herfurth, ZD 2018, S. 514 ff., mit einem Vorschlag entsprechender Kriterien; Hornung/Gilga, CR 2020, S. 367, Rn. 47 f., mit einer Systematisierung vorgeschlagener Abwägungskriterien; vgl. Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 64 mit Verweis auf fehlende Rechtssicherheit, die nur „geringfügig kompensiert“ wird; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 142 ff.; siehe bereits

Aufgrund des Anfangs sehr weiten Anwendungsbereichs und dem Erfordernis einer eigenverantwortlichen Konkretisierung durch den Verantwortlichen macht dies Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO – trotz entsprechender Kritik an eine solche Einordnung –<sup>96</sup> zu einer Art Generalklausel für Verarbeitungen, die nicht unter die, spezifischer definierten Rechtsgrundlagen fallen.<sup>97</sup>

#### d) Grafische Zusammenfassung

Die unterschiedlichen Ansätze, wie die Verarbeitungsinteressen für die Abwägung mit dem Interesse am Schutz personenbezogener Daten in den verschiedenen, gesetzlichen Rechtsgrundlagen festlegt werden, lassen sich grafisch wie folgt zusammenfassen:

---

zu Art. 7 DS-RL *Ferretti*, CML Rev. 51 (2014), p. 843, 858 f., mit Blick auf den damaligen Verordnungsvorschlag.

<sup>96</sup> Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 10, „kein Auffangtatbestand“; ähnlich Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 90; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 106, wobei seine Kritik an einer solchen Einordnung gerade den „selbstständigen und keineswegs nur nachrangigen“ Charakter der Rechtsgrundlage herausstellen möchte, der hier ebenfalls vertreten wird.

<sup>97</sup> Siehe Freund u.a./*Schmidt*, DSGVO, 2023, Art. 6 DS-GVO, Rn. 81, wonach die Einordnung als „Auffangtatbestand“ dem Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO faktisch zukommt; ebenfalls in diesem Sinne Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 64 f., der zwar gegen die Einordnung als (rechtliche) Generalklausel ist, sie aber aus faktischer Sicht als „Auffangtatbestand“ ansieht; ähnlich Schuster/Grützmaier/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 40. Siehe zur Einordnung als Generalklausel: Knyrim/*Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.73; Franzen/Gallner/*Oetker/Franzen*, EuArbRK, 5. Aufl. 2024, 270. Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 10; siehe auch Plath/*Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 53, „Auffangtatbestand“; auch als „Auffangtatbestand“ Schwartmann u.a./*Jacquemain u.a.*, DSGVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 136; ebenso Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 64; Specht/*Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 63; Kühling/*Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 141.

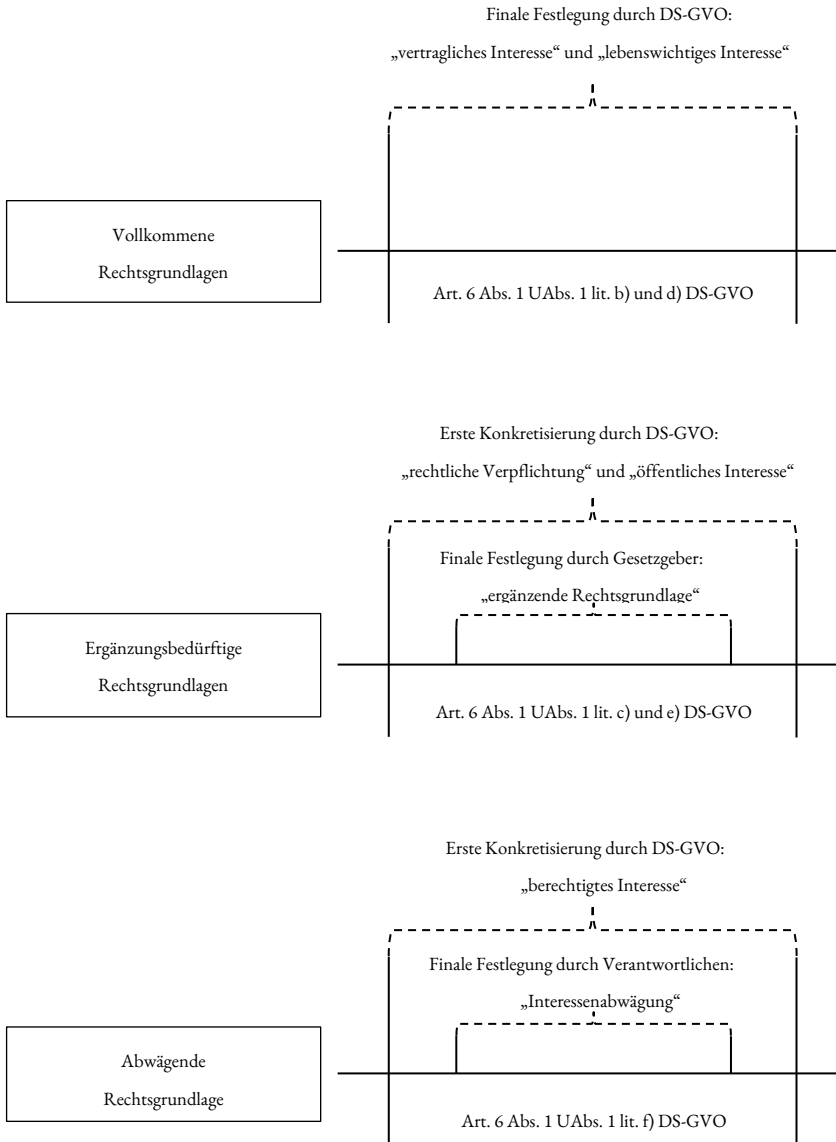


Abb. 6: Festlegung der Verarbeitungsinteressen für die Abwägung innerhalb der gesetzlichen Rechtsgrundlagen (eigene Darstellung)



### *3. Zwischenergebnis*

Die gesetzlichen Rechtsgrundlagen erlangen ihre Legitimation durch eine Abwägung der Interessen an einer Verarbeitung und den entgegenstehenden Interessen am Schutz vor einer solchen Verarbeitung. Der Ausgangspunkt liegt dabei auf Grundrechtsebene, da der Schutz personenbezogener Daten nicht absolut ist und auch (grundrechtlich) geschützte Interessen an einer Verarbeitung bestehen können.

Die gesetzlichen Rechtsgrundlagen nach Art. 6 Abs. 1 DS-GVO bilden diese Interessenabwägung ab, wobei es innerhalb der Rechtsgrundlagen drei Ansätze für diese Interessenabwägung gibt. Bei den vollkommenen Rechtsgrundlagen wurde die Interessenabwägung von der Datenschutz-Grundverordnung selbst abschließend vorgenommen. Die ergänzungsbedürftigen Rechtsgrundlagen übertragen diese Aufgabe an den Gesetzgeber einer hierfür erforderlichen ergänzenden Rechtsgrundlage. Die abwägende Rechtsgrundlage hingegen überträgt die Aufgabe der Abwägung auf den Verantwortlichen selbst.

### *IV. Zwischenergebnis*

Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten basieren auf unterschiedlichen Legitimationsgedanken und prägen somit ihren jeweiligen Anwendungsbereich. Grob kann unterschieden werden zwischen der Einwilligung und den gesetzlichen Rechtsgrundlagen. Die Einwilligung erlangt ihre Legitimation durch die Zustimmung der betroffenen Person in die Verarbeitung ihrer Daten. Daher konzentrieren sich die Anforderungen an eine wirksame Einwilligung darauf, den selbstbestimmenden Charakter dieser Zustimmung zu gewährleisten. Die Kontrolle der Rechtmäßigkeit der Verarbeitung zu einem bestimmten Zweck übernimmt damit die betroffene Person selbst, indem sie die Verarbeitung mit ihrer Zustimmung für rechtmäßig erklärt.

Bei den gesetzlichen Rechtsgrundlagen hat der Gesetzgeber vorab eine Entscheidung darüber getroffen, in welchen Bereichen das Interesse an einer Datenverarbeitung dem Schutzinteresse der betroffenen Person überwiegt. Der Legitimationsgedanke der gesetzlichen Rechtsgrundlagen fußt dabei auf dem Gedanken, dass der Schutz betroffener Personen vor einer Verarbeitung ihrer Daten nicht absolut ist. Die Anwendungsfelder, in denen das Verarbeitungsinteresse überwiegt, werden durch die Vorgabe eines Zweckrahmens eingegrenzt.

Bei sehr weitreichenden Zweckrahmen kennt die Verordnung verschiedene Instrumente, diese weiter einzugrenzen.

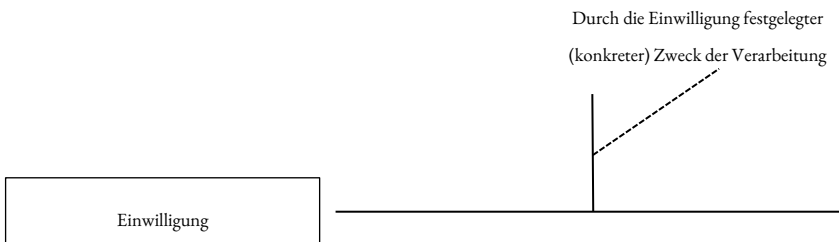
Doch was bedeutet dies nun für die Rechtmäßigkeit einer Datenverarbeitung und der Auswahl einer geeigneten Rechtsgrundlage?

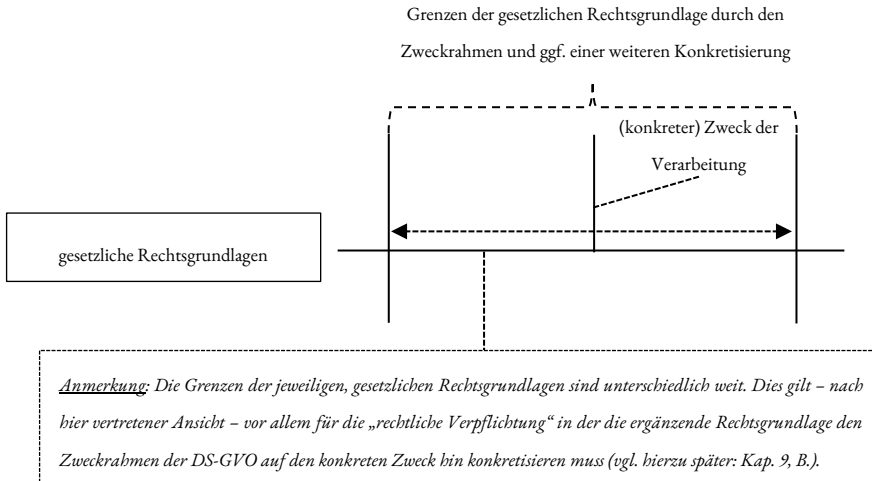
## D. Schlussfolgerung

Ausgangspunkt ist die Festlegung eines konkreten Verarbeitungszwecks durch den Verantwortlichen i.S.d. Zweckbindungsgrundsatzes nach Art. 5 Abs. 1 lit. b) DS-GVO. Nach der Zweckfestlegung ist zu prüfen, ob und wenn ja welche Rechtsgrundlage diesen konkreten Zweck der Verarbeitung umfasst. Hier kommt dann u.a. der Zweckrahmen der gesetzlichen Rechtsgrundlagen zur Anwendung. Fällt der konkrete Zweck in den vordefinierten Zweckrahmen einer gesetzlichen Rechtsgrundlage, kommt diese Rechtsgrundlage für die Verarbeitung grundsätzlich in Frage. Liegen dann zusätzlich noch die weiteren Voraussetzungen der jeweiligen Rechtsgrundlage vor, ist die Verarbeitung rechtmäßig und der Verantwortliche kann die Verarbeitung vornehmen.

Im Falle der Einwilligung kann der Verantwortliche u.a. unter Angabe des konkreten Verarbeitungszwecks die betroffene Person um ihre Zustimmung zur Datenverarbeitung bitten. Die betroffene Person kann dann direkt über den konkreten Zweck der Verarbeitung entscheiden und mit ihrer Einwilligung die Verarbeitung für rechtmäßig erklären.

Die nachfolgende Darstellung verdeutlicht noch einmal grafisch das Verhältnis zwischen Zweck und Zweckrahmen und die Vorgehensweise bei der Auswahl einer Rechtsgrundlage:





*Abb. 7: Verhältnis von Zweck und Zweckrahmen bei der Auswahl einer Rechtsgrundlage (eigene Darstellung)*



## Kapitel 9

# Rechtsgrundlage für datenverarbeitende TOM

Nach dem System des europäischen Datenschutzrechts bedarf es für jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage.<sup>1</sup> Dies gilt demnach auch für datenverarbeitende TOM bzw. die ihnen jeweils zugrundeliegende Datenverarbeitung. Welche Rechtsgrundlage für datenverarbeitende TOM einschlägig ist, kann dabei nur schwer pauschal gesagt werden, da dies immer von dem jeweiligen Zweck der Verarbeitung abhängt.<sup>2</sup> Der Zweck der Verarbeitung muss dabei entweder in den Zweckrahmen einer der gesetzlichen Rechtsgrundlagen fallen oder von einer Einwilligung abgedeckt sein.<sup>3</sup>

### A. Die Sicherheit der Verarbeitung als Verarbeitungszweck?

Denkbar wäre es, in der Sicherheit der Verarbeitung, wie sie in Art. 32 DS-GVO beschrieben ist, den Zweck der Verarbeitung durch datenverarbeitende TOM zu sehen. Damit würden alle datenverarbeitenden TOM denselben Zweck verfolgen, was eine Subsumtion unter eine (gemeinsame) Rechtsgrundlage vereinfachen könnte. Wenn man sich noch einmal vergegenwärtigt, dass der Zweck den Grund beschreibt, warum eine Verarbeitung personenbezogener Daten vorgenommen werden soll, dann könnte man auch argumentieren, dass datenverarbeitende TOM schließlich die Sicherheit der Verarbeitung nach Art. 32 DS-GVO gewährleisten sollen und es sich bei der Sicherheit der Verarbeitung somit um den Verarbeitungszweck handelt. Die Gewährleistung der Sicherheit

---

<sup>1</sup> Siehe hierzu: Kap. 2, A., II. *Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO* und Kap. 8, A. *Die Notwendigkeit einer Rechtsgrundlage*.

<sup>2</sup> Siehe hierzu: Kap. 8, B. *Ausrichtung am Zweck der Verarbeitung*.

<sup>3</sup> Siehe hierzu: Kap. 8, D. *Schlussfolgerung*.

der Verarbeitung nach Art. 32 DS-GVO hängt jedenfalls mit Grund für die Verarbeitung zusammen.

Fraglich bleibt aber, ob die Sicherheit der Verarbeitung als Zweck auch hinreichend bestimmt ist. Hierzu müssen die Anforderungen nach Art. 5 Abs. 1 lit. b) DS-GVO gegeben sein. Der Zweck muss derart bestimmt sein, dass aus ihm klar hervorgeht, wofür die Daten verarbeitet werden sollen.<sup>4</sup>

Zu allgemein und damit für einen konkreten Zweck untauglich sind daher Angaben wie „Marketing“<sup>5</sup>, IT-Sicherheit<sup>6</sup> oder „Produktverbesserung“<sup>7</sup>.<sup>8</sup>

Problematisch könnte in diesem Zusammenhang sein, dass es keine einheitlichen Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-

---

<sup>4</sup> Vgl. BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 15; Kühling/Buchner/*Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 5 DS-GVO, Rn. 35; Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 14; siehe auch *Spies*, ZD 2022, S. 75, 76, der jedoch in Abhängigkeit von der „Eingriffsintensität“ die Anforderungen an die Bestimmtheit weiter ausrichten möchte; ähnlich auch *Ziegenborn/Schulz-Große*, ZD 2023, S. 581, 583 f., die die Anforderungen an die Bestimmtheit des Zwecks anhand des Einzelfalls unter Berücksichtigung der Verhältnismäßigkeit bestimmen wollen.

<sup>5</sup> *Simitis/Hornung/Spiecker* gen. *Döhmman/Roßnagel*, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 88; *DatKomm/Hötzendorfer/Tschobl/Kastelitz*, Stand: 76. EL. 2023, Art. 5 DS-GVO (Stand: Juli 2020), Rn. 26; *Knyrim/Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.10; BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 15, „Werbung“; auch *Specht/Mantz/Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 86.

<sup>6</sup> BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 15; *DatKomm/Hötzendorfer/Tschobl/Kastelitz*, Stand: 76. EL. 2023, Art. 5 DS-GVO (Stand: Juli 2020), Rn. 26; *Knyrim/Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.10; *Specht/Mantz/Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 86.

<sup>7</sup> BeckOK Datenschutzrecht/*Schantz*, Stand: 46. Ed. 2023, Art. 5 DS-GVO (Stand: November 2021), Rn. 15, „Verbesserung der Leistung“; *DatKomm/Hötzendorfer/Tschobl/Kastelitz*, Stand: 76. EL. 2023, Art. 5 DS-GVO (Stand: Juli 2020), Rn. 26, „Verbesserung der Benutzerfreundlichkeit“; auch *Knyrim/Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.10; ähnlich *Specht/Mantz/Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 86.

<sup>8</sup> Diese Beispiele wurden so oder so ähnlich bereits von der früheren Artikel-29-Gruppe, WP 203, S. 16 – auf die sich die Literatur noch stützt – als nicht ausreichend für die konkrete Zweckfestlegung angesehen. Der Europäische Datenschutzausschuss hat diese Stellungnahme jedoch nicht offiziell gebilligt.

GVO gibt. Die Gewährleistung der Sicherheit der Verarbeitung richtet sich nach dem jeweiligen Einzelfall. Es gibt somit nicht die eine Sicherheit.<sup>9</sup>

Man könnte dies vergleichen mit der Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO. Danach können vertragliche Interessen eine Datenverarbeitung legitimieren. Das in Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO beschriebene Vertragsinteresse allgemein stellt jedoch nicht den (konkreten) Zweck der Verarbeitung dar bzw. reicht es für die Zweckfestlegung nicht aus, lediglich auf die Rechtsgrundlage zu verweisen.<sup>10</sup> Es kommt vielmehr auf den konkreten Vertrag und nicht irgendein theoretisch denkbare Vertragsinteresse an.<sup>11</sup>

Dies müsste dann auch für die Sicherheit der Verarbeitung i.S.d. Art. 32 DS-GVO gelten. Ein Verweis auf die allgemeine Sicherheit nach Art. 32 DS-GVO dürfte ebenfalls nicht den Bestimmtheitsanforderungen eines konkreten Zwecks i.S.d. Art. 5 Abs. 1 lit. b) DS-GVO genügen. Auch hier käme es für die Festlegung eines konkreten Zwecks auf die Gewährleistung der jeweiligen Sicherheit der Verarbeitung an. Im Gegenzug wäre dann – in der hier vorgenommenen Differenzierung – die allgemeine Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DS-GVO eher als Zweckrahmen anzusehen.

---

<sup>9</sup> Siehe hierzu: Kap. 5, A. *Risikobewertung*.

<sup>10</sup> Siehe allgemein dazu, dass ein Verweis auf die Rechtsgrundlagen nicht ausreichend ist: Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 5 DS-GVO, Rn. 22; Spies, ZD 2022, S. 75, 76; Simitis/Hornung/Spiecker gen. Döhmann/Roßnagel, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 87; vgl. Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 402; siehe bereits Roßnagel/Nebel/Richter, ZD 2015, S. 455, 457 f., noch zum Gesetzgebungsverfahren, die bei einer Gleichsetzung des „*eindeutige[n] Zweck[s]*“ mit den Erlaubnistatbeständen eine wirksame Zweckbindung anzweifeln.

<sup>11</sup> Vgl. zum Verweis auf den konkreten Vertrag, allerdings im Zusammenhang der Erforderlichkeit: Simitis/Hornung/Spiecker gen. Döhmann/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 29; Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 13; Klein, Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?, in: FS Taeger, 2020, S. 235, 246 f., Schulze/Janssen/Kadelbach/Holz-nagel/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 22; Moos/Schefzig/Arning/Arning, Praxis-handbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 47; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 39; Wybitul/Pötters/Rauer, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 15, „*konkreten Vertragszweck*“.

## B. Art. 32 DS-GVO als ergänzende Rechtsgrundlage

Ausgehend von dieser Einordnung knüpft keine der Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO unmittelbar an einen Zweckrahmen wie die Sicherheit der Verarbeitung an. Für datenverarbeitende TOM könnte allerdings überlegt werden, ob Art. 32 DS-GVO als eine rechtliche Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO angesehen werden kann und damit als eine ergänzende Rechtsgrundlage einzuordnen ist. Wie bereits oben kurz beschrieben, müsste Art. 32 DS-GVO hierbei vor allem die Anforderungen des Art. 6 Abs. 3 DS-GVO erfüllen.<sup>12</sup> Als Teil der Datenschutz-Grundverordnung und damit Teil des Unionsrechts (vgl. Art. 6 Abs. 3 S. 1 lit. a) DS-GVO), dürfte es sich bei Art. 32 DS-GVO grundsätzlich um eine denkbare, ergänzende Rechtsgrundlage für eine rechtliche Verpflichtung handeln.<sup>13</sup>

### *I. „Verpflichtung“ zur Verarbeitung personenbezogener Daten nach Art. 32 DS-GVO*

Weiters wird für die Einordnung als ergänzende Rechtsgrundlage vorausgesetzt, dass sich die Rechtsgrundlage unmittelbar auf eine Verarbeitung personenbezogener Daten bezieht.<sup>14</sup> Nicht ausreichend soll es sein, dass zur Erfüllung einer

<sup>12</sup> Siehe hierzu: Kap. 8, C., III., 2., b) *Ergänzungsbedürftige Rechtsgrundlagen*.

<sup>13</sup> Zu der Frage, ob die Datenschutz-Grundverordnung selbst als ergänzende Rechtsgrundlage dienen kann: Zustimmung *Piltz*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnisstatbestand, in: FS Taeger, 2020, S. 351, 353, konkret zu Art. 32 DS-GVO; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 42; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 81; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 83a, verweisen allgemein auf die Datenschutz-Grundverordnung; auch allgemein auf die DS-GVO verweisend Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 59. A.A. wohl *Spies*, ZD 2022, S. 75, 79, mit dem Verweis auf eine Rechtsgrundlage „*außerhalb der DS-GVO*“.

<sup>14</sup> LSG Hessen, BeckRS 2020, 1442, Rn. 13; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 48; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 76; Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 595; Knyrim/*Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.79; ähnlich wohl auch Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 74, wonach es nicht ausreichen soll, wenn „*die Vorschrift die Datenverarbeitung nur voraussetzt, aber selbst nicht anordnet*“; vgl. Specht/Mantz/*Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3,



Verpflichtung auch personenbezogene Daten verarbeitet werden müssen.<sup>15</sup> Diese Anforderung kann für die Einordnung des Art. 32 DS-GVO als eine rechtliche Verpflichtung ein besonderes Problem darstellen.

Denn ausgehend vom Regelungsgehalt schreibt Art. 32 DS-GVO unmittelbar keine Datenverarbeitung vor.<sup>16</sup> Art. 32 DS-GVO verlangt die Gewährleistung eines angemessenen Schutzniveaus. Lediglich faktisch kann es vorkommen, dass bei der Umsetzung mittels technischer und organisatorischer Maßnahmen auch personenbezogene Daten verarbeitet werden. Die Verarbeitung personenbezogener Daten bei der Gewährleistung der Sicherheit stellt zwar keine Ausnahme dar, dürfte aber auch nicht immer zwingend sein.<sup>17</sup> Daher stellt sich die Frage, ob der Bezug einer ergänzenden Rechtsgrundlage auf eine Datenverarbeitung unmittelbar aus dem Wortlaut der Rechtsgrundlage hervorgehen muss oder ob es ausreichend ist, dass sich dieser Bezug auch aus der Vorschrift ableiten lässt.<sup>18</sup>

Ob sich die Datenverarbeitung unmittelbar aus dem Wortlaut einer Vorschrift ergeben muss oder nicht, um als ergänzende Rechtsgrundlage eingeordnet zu werden, geht aus den Anforderungen des Art. 6 Abs. 3 DS-GVO nicht hervor.<sup>19</sup> Anhaltspunkte könnten sich hier aber vor allem aus der Funktion der

---

Rn. 60; *Deusch/Eggendorfer*, Intrusion Detection und DSGVO, in: Rechtsfragen digitaler Transformationen, 2018, S. 741, 749.

<sup>15</sup> LSG Hessen, BeckRS 2020, 1442, Rn. 13; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 48; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 76; Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 595.

<sup>16</sup> *Piltz*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 353; *Poncza*, ZD 2023, S. 8, 11; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 81; siehe auch Freund u.a./*Schmidt*, DSGVO, 2023, Art. 6 DS-GVO, Rn. 49 f. allgemein zu „Pflichtbegründenden Normen“ (mit Art. 32 DS-GVO als Beispiel) der Datenschutz-Grundverordnung.

<sup>17</sup> Siehe hierzu: Kap. 2, C. *Die Bedeutung datenverarbeitender TOM*.

<sup>18</sup> Dieser Frage widmet sich ausführlich *Piltz*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 353 ff. in Bezug auf Art. 32 DS-GVO., mit dem Ergebnis, dass eine Ableitung einer Datenverarbeitung aus der Vorschrift ausreicht (S. 355); ähnlich auch zu Art. 32 DS-GVO *Poncza*, ZD 2023, S. 8, 11; a.A. u.a. zu Art. 32 DS-GVO Freund u.a./*Schmidt*, DSGVO, 2023, Art. 6 DS-GVO, Rn. 50.

<sup>19</sup> *Poncza*, ZD 2023, S. 8, 11; A.A. wohl *Piltz*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 355, mit Verweis auf die Differenzierung zwischen den zwingenden und fakultativen Anforderungen nach Art. 6 Abs. 3 DS-GVO und einer

ergänzenden Rechtsgrundlagen und ihrer Legitimation ergeben. Die ergänzenden Rechtsgrundlagen dienen als Verbindung zwischen dem Datenschutzrecht und anderen Rechtsgebieten und sollen Datenverarbeitungen in anderen Rechtsgebieten datenschutzrechtliche Geltung verschaffen.<sup>20</sup>

Dabei darf man aber nicht vergessen, dass der originäre Anwendungsbereich ergänzender Rechtsgrundlagen nicht in der Legitimation von Datenverarbeitungen liegt. Vorrangig regeln diese Vorschriften ihre entsprechenden eigenen Regelungsbereiche. Erst durch den Verweis des Art. 6 Abs. 3 DS-GVO können sie gleichzeitig als datenschutzrechtliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen.<sup>21</sup> Damit kann von ergänzenden Rechtsgrundlagen allerdings nicht verlangt werden, dass sie – gerade weil sie kein originäres Datenschutzrecht sind – auch eine Datenverarbeitung unmittelbar vorschreiben.<sup>22</sup> Es muss ausreichen, dass sich eine Datenverarbeitung aus der Vorschrift ableiten lässt.<sup>23</sup>

Das Art. 32 DS-GVO daher keine Verarbeitung personenbezogener Daten ausdrücklich verlangt, sollte einer Einordnung als ergänzende Rechtsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) i.V.m. Abs. 3 DS-GVO nicht entgegenstehen.<sup>24</sup>

---

fehlenden, zwingenden Anforderung an die Spezifizierung der Verarbeitung in einer ergänzenden Rechtsgrundlage.

<sup>20</sup> Siehe hierzu: Kap. 8, C., III., 2., b) *Ergänzungsbedürftige Rechtsgrundlagen*.

<sup>21</sup> Vgl. Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 592, wonach diese Vorschriften „in Datenschutzrecht transformiert werden“, zudem verweist er (vorrangig jedoch aufgrund des Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO) darauf, dass sie andernfalls „keine Rechtsgrundlagen iSd DS-GVO“ darstellen (Rn. 597).

<sup>22</sup> Vgl. Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 60, „nicht zwangsläufig eine datenschutzrechtliche Erlaubnisnorm im klassischen Sinne sein“.

<sup>23</sup> So im Ergebnis Piltz, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 355 und im Rahmen des Art. 32 DS-GVO; auch Poncza, ZD 2023, S. 8, 11, anhand von Art. 32 DS-GVO; ähnlich Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 81, ebenfalls am Beispiel des Art. 32 DS-GVO; allgemein, aber wohl auch Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 60; allgemein a.A. Knyrim/Haidinger, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.80, die dann auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO verweist; ähnlich Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 595 f.; ebenfalls a.A. Freund u.a./Schmidt, DSGVO, 2023, Art. 6 DS-GVO, Rn. 50.

<sup>24</sup> Piltz, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 355; Poncza, ZD 2023, S. 8, 11; Taeger/Gabel/Taeger, DSGVO – BDSG –

## II. Anforderungen an den Zweck der Verarbeitung

Nach hier vertretener Ansicht scheitert eine Einordnung der Gewährleistung der Sicherheit der Verarbeitung als rechtliche Verpflichtung und damit als ergänzende Rechtsgrundlage jedenfalls nicht daran, dass Art. 32 DS-GVO eine Datenverarbeitung nicht unmittelbar vorschreibt.

Problematischer erscheint vielmehr der Konkretisierungsgrad des Art. 32 DS-GVO hinsichtlich des Zwecks der Verarbeitung. Gem. Art. 6 Abs. 3 S. 2 Alt. 1 DS-GVO<sup>25</sup> muss die ergänzende Rechtsgrundlage den Zweck der Verarbeitung festlegen.<sup>26</sup> Im Vergleich zur zweiten Alternative, die sich ausschließlich auf ergänzende Rechtsgrundlagen i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO bezieht,<sup>27</sup> ist hierfür wohl Voraussetzung, dass die Rechtsgrundlage bereits den

---

TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 81; wohl im Ergebnis auch Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 42, der unter Verweis auf Piltz Art. 32 DS-GVO als ergänzende Rechtsgrundlage einordnet; a.A. Freund u.a./Schmidt, DSGVO, 2023, Art. 6 DS-GVO, Rn. 50, u.a. mit Art. 32 DS-GVO als Beispiel.

<sup>25</sup> Art. 6 Abs. 3 DS-GVO wird stellenweise anders zitiert. Anstatt S. 1 wird dieser als UAbs. 1 gesehen, wodurch S. 2 ff. zu UAbs. 2 S. 1 ff. werden (siehe bspw. Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, die Überschriften für die Rn. 38 ff.).

<sup>26</sup> Piltz, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 356; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 161; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 80; Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 29; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 93; Knyrim/Haidinger, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.70; Specht/Mantz/Mantz/Marosi, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 60; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 60.

<sup>27</sup> Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 41, 66; Specht/Mantz/Mantz/Marosi, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 62; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 162; vgl. Knyrim/Haidinger, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.72; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 91; so ausgehend vom Wortlaut auch Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 29, aber aufgrund (wohl) teleologischer Erwägungen im Ergebnis ablehnend. Siehe auch Spies, ZD 2022, S. 75, 79 f., mit einer abweichenden Wortlautauslegung hinsichtlich des „oder“ der beiden Alternativen.

konkreten Zweck festlegt.<sup>28</sup> Eine Konkretisierung mittels eines Zweckrahmens, dürfte in den Fällen des Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO nicht möglich sein (wohl aber für die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO)<sup>29</sup>. Die Differenzierung zwischen den ergänzenden Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e) DS-GVO dürfte darauf zurückzuführen sein, dass eine rechtliche Verpflichtung i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO eben eine Verpflichtung ausspricht, der nachzukommen ist.<sup>30</sup> Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO ist hierauf nicht beschränkt, sondern kann ge-

<sup>28</sup> Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 91; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 41; Gierschmann u.a./*Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 162; *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 392, 404; Simitis/Hornung/Spiecker gen. Döhmann/*Rofsnagel*, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 29 verlangt für beide Fälle die Festlegung des konkreten Zwecks. Siehe auch im Umkehrschluss, aber sprachlich etwas weit Knyrim/*Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.72, wonach der Zweck für Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO „entfallen [kann]“.

<sup>29</sup> Siehe auch Gierschmann u.a./*Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 162, die für Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO eine „generalklauselartig formulierte Rechtsgrundlage“ genügen lassen. A.A. wohl Simitis/Hornung/Spiecker gen. Döhmann/*Rofsnagel*, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 29 der einen Zweckrahmen für lit. e) ablehnen dürfte, da er in beiden Fällen die Festlegung des Zwecks in der gesetzlichen Regelung verlangt; ihm schließt sich *Spies*, ZD 2022, S. 75, 79 wohl weitgehend an, dürfte die Auswirkungen aber später (Rn. 80) hinsichtlich der Bestimmtheit der Festlegung etwas relativieren.

<sup>30</sup> Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 37; Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 58; siehe auch Taeger/*Gabel/Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 75, wonach eine „Erlaubnis“ – im Vergleich zur Datenschutzrichtlinie – nicht mehr ausreiche, solche aber dann wohl von Art. 6 Abs. 1 UAbs. 1 lit. e) und f) DS-GVO umfasst sein könnte; vgl. auch Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 53, der „erlaubende Rechtsvorschriften“ ausschließt; ähnlich Plath/*Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 42; so wohl auch Knyrim/*Haidinger*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 5.80; Kuner/*Bygrave/Docksey/Kotschy*, GDPR, 2020, p. 333; Forgó/*Helfrich/Schneider/Hanloser*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V, Kapitel 1, Rn. 20, „ohne Entschließungs- bzw. Handlungsermessens“.

rade auch für den Verantwortlichen eine Erlaubnis sein, die Daten zu verarbeiten.<sup>31</sup> Hiermit verbunden ist ein gewisser Ermessenspielraum, der von dem Verantwortlichen noch auszufüllen ist.<sup>32</sup>

Während es für ergänzende Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO daher eines konkreten Zwecks bedarf, dürfte es in den Fällen des Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO auch ausreichen, wenn ein Zweckrahmen für die Rechtsgrundlage definiert wird. Der konkrete Zweck müsste dann – wie sonst auch –<sup>33</sup> vom Verantwortlichen noch festgelegt werden und muss sich im Rahmen des Zweckrahmens der ergänzenden Rechtsgrundlage bewegen.

Daher muss auch bereits der Zweck der Verarbeitung (also die Verpflichtung) in der Rechtsgrundlage festgelegt sein. Aufgrund des Ermessenspielraums im Falle des Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO darf dort hingegen der Zweck abstrakter sein, also durch die Definition eines Zweckrahmens erfolgen. Der konkrete Zweck muss dann von dem Verantwortlichen festgelegt werden, der sein Ermessen durch die Rechtsgrundlage damit ausübt.

Wie bei der Verpflichtung zur Datenverarbeitung dürfte von einer ergänzenden Rechtsgrundlage nicht verlangt werden, dass diese den Zweck der Verarbeitung i.S.d. Datenschutzrechts ausdrücklich als solchen benennen muss, sondern

---

<sup>31</sup> Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 65; vgl. Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 15, „Befugnisse mit einem Ermessens- oder Beurteilungsspielraum einräumen“; siehe auch Kuner/Bygrave/Docksey/Kotschy, GDPR, 2020, p. 336, spricht von einer „*more general authorisation to act*“ im Vergleich zu Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO, siehe zudem die Einschränkung zu lit. c) (p. 333). Siehe auch die Abgrenzung zwischen Art. 6 Abs. 1 UAbs. 1 lit. c) und e) bei Forgó/Helfrich/Schneider/Hanloser, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V, Kapitel 1, Rn. 20.

<sup>32</sup> Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 65; vgl. Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 15, „Ermessens- oder Beurteilungsspielraum“; siehe auch Kuner/Bygrave/Docksey/Kotschy, GDPR, 2020, p. 336, die aufgrund der „Auslegung und Abwägungen von Interessen“ eine Gemeinsamkeit des Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO mit Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO und auch deren Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO sieht. Wohl auch Forgó/Helfrich/Schneider/Hanloser, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V, Kapitel 1, Rn. 20, der gerade im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO auf ein fehlendes „*Entschließungs- bzw. Handlungsermessen*“ verweist und damit eine Abgrenzung zu Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO vornimmt.

<sup>33</sup> Siehe hierzu bereits grob skizziert: Kap. 8, D. *Schlussfolgerung*.

dass sich auch hier der konkrete Zweck der Verarbeitung aus der Rechtsgrundlage ableiten lassen kann.<sup>34</sup>

Bezogen auf Art. 32 DS-GVO dürfte hier jedoch problematisch sein, dass es nicht die eine Sicherheit der Verarbeitung gibt. Die Anforderungen und damit die konkrete Umsetzung (was sich letztlich auf den Zweck der Verarbeitung durchschlägt) sind am Einzelfall zu bestimmen. Daher dürfte dem Art. 32 DS-GVO wohl allenfalls ein Zweckrahmen zugrunde liegen und eben kein konkreter Verarbeitungszweck.<sup>35</sup> Damit scheidet eine Einordnung des Art. 32 DS-GVO als ergänzende Rechtsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) i.V.m. Abs. 3 DS-GVO nach hier vertretener Ansicht aus.<sup>36</sup>

Auch eine Einordnung als Aufgabe in einem öffentlichen Interesse oder gar die Ausübung öffentlicher Gewalt dürfte – gerade für den hier betrachteten unternehmerischen Kontext –<sup>37</sup> nicht einschlägig sein.

---

<sup>34</sup> Piltz, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 356; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 41; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 93 „implizite Zweck“; ähnlich auch Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 215, „Erkennbarkeit des impliziten Zwecks“.

<sup>35</sup> Siehe hierzu bereits: Kap. 9, A. Die Sicherheit der Verarbeitung als Verarbeitungszweck?.

<sup>36</sup> Im Ergebnis auch gegen eine Einordnung als Rechtsgrundlage des Art. 32 DS-GVO i.V.m. Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO Schuster/Grützmacher/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 7 und will aber wohl die Verarbeitung nach Art. 32 DS-GVO gemeinsam mit der „primären Datenverarbeitung“ (wohl die nach Art. 32 DS-GVO zu schützende Verarbeitung) behandeln; so auch Freund u.a./Schmidt, DSGVO, 2023, Art. 6 DS-GVO, Rn. 50. A.A. Piltz, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351, 356 f., 359, der jedenfalls die Anforderung an den Zweck in Art. 32 DS-GVO als erfüllt ansieht; auch Poncza, ZD 2023, S. 8, 11 sieht die Anforderungen an den Zweck in Art. 32 DS-GVO (konkret am Beispiel für Penetrationstest, insbesondere auch durch Art. 32 Abs. 1 Hs. 2 lit. d) DS-GVO) erfüllt. Siehe auch die Einschätzung von GA Kokott, Schlussanträge v. 08.05.2008 zur Rs. C-73/07 (Satakunnan Markkinapörssi und Satamedia), ECLI:EU:C:2008:266, Rn. 112, zu Art. 17 Abs. 1 DS-RL (heute vergleichbar mit Art. 32 DS-GVO), wonach dieser „die Rechtmäßigkeit der Datenverarbeitung [...] nicht [...] regelt“, wobei die Ausführungen allerdings offenlassen, ob Art. 17 Abs. 1 DS-RL im Zusammenhang mit Art. 7 lit. c) und e) DS-RL (heute Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO) bzw. deren Umsetzungen im nationalen Recht gesehen werden kann.

<sup>37</sup> Siehe zur entsprechenden Themeneingrenzung dieser Arbeit: Kap. 3, C., II. Beschränkung auf den unternehmerischen Bereich.

## C. Die Frage einschlägiger Rechtsgrundlagen

Die Einordnung des Art. 32 DS-GVO als ergänzende Rechtsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) i.V.m. Abs. 3 DS-GVO und damit eine Subsumtion datenverarbeitender TOM hierunter, ist durchaus fraglich und wird nach hier vertretener Ansicht abgelehnt. Dies wirft das Problem nach möglichen Alternativen auf.

### *I. Anforderungen an die „Auswahl“ einer geeigneten Rechtsgrundlage*

Fraglich ist allerdings, ob es an dieser Stelle bereits einer Festlegung auf eine bestimmte Rechtsgrundlage für die weitere Untersuchung bedarf. Denn solange die Verarbeitung von einer Rechtsgrundlage abgedeckt ist, ist diese Verarbeitung rechtmäßig. Die Datenschutz-Grundverordnung differenziert bei der Rechtsfolge also nicht zwischen den einzelnen Rechtsgrundlagen.<sup>38</sup> Insofern könnte man die Frage der Festlegung auf eine bestimmte Rechtsgrundlage auch vom späteren Einzelfall abhängig machen, wodurch dieser Frage hier nur eine nachrangige Bedeutung zukommen würde. Problematisch wäre dies allerdings, wenn die Datenschutz-Grundverordnung bereits vorab bestimmte Eingrenzungen vornimmt, die es hier zu beachten gälte. Um dies ausschließen zu können, muss daher zunächst geklärt werden, welche Anforderungen die Datenschutz-Grundverordnung an die „Auswahl“ einer geeigneten Rechtsgrundlage stellt.

---

<sup>38</sup> Vgl. VG Mainz, BeckRS 2020, 5397, Rn. 27, „die in Art. 6 Abs. 1 DSGVO enthaltenen Zulässigkeitstatbestände ihrer rechtlichen Funktion nach gleichwertig“; auch Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 10; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 7, „alle die gleiche auf die Zulässigkeit abzielende Funktionalität“; Knyrim/Wyrobek, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 6.1.

Die Verordnung verlangt, dass „*mindestens eine*“<sup>39</sup> Rechtsgrundlage vorliegt, vgl. Art. 6 Abs. 1 UAbs. 1 DS-GVO.<sup>40</sup> Im Umkehrschluss<sup>41</sup> bedeutet das, dass eine Datenverarbeitung daher auch grds. von mehreren Rechtsgrundlagen gleichzeitig erfasst werden kann.<sup>42</sup> Die Rechtsgrundlagen stehen daher nicht in

<sup>39</sup> Englisch: „*at least one*“, Französisch: „*au moins une*“, Spanisch: „*al menos una*“, Italienisch: „*almeno una*“, Niederländisch: „*minste een*“.

<sup>40</sup> Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 18; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 13a, 22; Plath/*Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 6; Paal/*Pauly/Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 3; Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 7; Spindler/Schuster/*Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 2; Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 1; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 6; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 21; Kuner/Bygrave/Docksey/*Kotschy*, GDPR, 2020, p. 329; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 6, 24.

<sup>41</sup> Konkret auf das Argumentationsmittel des „Umkehrschluss“ abstellend: Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 7. Siehe allgemein zum Umkehrschluss (*argumentum e contrario*) als Argumentationsmittel: EuGH, Rs. C-434/08 (Harms), ECLI:EU:C:2010:285 = BeckRS 2010, 90607, Rn. 44; EuGH, Rs. C-339/17 (Verein für lauterer Wettbewerb), ECLI:EU:C:2018:539 = GRUR 2018, S. 1061, Rn. 37; EuGH, Rs. C-754/18 (Ryanair Designated Activity Company), ECLI:EU:C:2020:478 = BeckRS 2020, 12792, Rn. 27; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 143; Beck, The Legal Reasoning of the Court of Justice of the EU, 2012, pp. 221 f.; Martens, Methodenlehre des Unionsrechts, 2013, S. 327 f.; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 34, siehe zu den Argumentationsmitteln aber auch den Verweis auf andere Werke dort in Fn. 136.

<sup>42</sup> Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 7, 141; Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 18; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 13a, 22; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 21; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 9; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (August 2023), Rn. 6, 24; Plath/*Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 6; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 6; Paal/*Pauly/Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 8; Krusche, ZD 2020, S. 232, 233 f.; Kollmar/*El-Auwad*, K&R 2021, S. 73, 77.



einem Ausschließlichkeitsverhältnis zueinanderstehen und auch eine Kumulation ist möglich.<sup>43</sup> Voraussetzung ist jedoch, dass die spezifischen Anforderungen der jeweiligen Rechtsgrundlage erfüllt sind.<sup>44</sup>

Auch wenn die Datenschutz-Grundverordnung es nicht ausschließt, dass eine Datenverarbeitung gleichzeitig unter mehrere Rechtsgrundlagen fallen kann, beantwortet dies noch nicht die Frage, ob der Verantwortliche dann auch nach Belieben auf die einzelnen Rechtsgrundlagen zurückgreifen kann. Dies wäre nicht möglich, wenn den Rechtsgrundlagen ein besonderes Rangverhältnis zugrunde liegen würde, dass den Verantwortlichen dazu zwänge auf bestimmte Rechtsgrundlagen vor- oder nachrangig zurückzugreifen.

Eine gesetzlich angeordnete Rangfolge lässt sich jedenfalls nicht aus der Reihenfolge ableiten, in der die Rechtsgrundlagen in Art. 6 Abs. 1 DS-GVO aufgelistet sind.<sup>45</sup> Somit kommt der Einwilligung (als die erst genannte Rechtsgrundlage) im Verhältnis zu den darauffolgenden Rechtsgrundlagen keine höhere

---

<sup>43</sup> Zur Möglichkeit der Kumulation: *Krusche*, ZD 2020, S. 232, 233 ff.; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 8; Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 141; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 24; *Kollmar/El-Auwad*, K&R 2021, S. 73, 77; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 9; *Schneider*, Datenschutz, 2. Aufl. 2019, S. 109.

<sup>44</sup> Vgl. Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 8; siehe auch EuGH, Rs. C-398/15 (Manni), ECLI:EU:C:2017:197 = BeckRS 2017, 103300, Rn. 42, noch zum vergleichbaren Art. 7 DS-RL unter Verweis auf die Schlussanträge des Generalanwalts *GA Bot*, Schlussanträge v. 08.09.2016 zur Rs. C-398/15 (Manni), ECLI:EU:C:2016:652 = BeckRS 2016, 82240, Rn. 52. Siehe auch *Feiler/Forgó*, EU-DSGVO und DSGVO, 2. Aufl. 2022, Art. 6 DS-GVO, Rn. 2, die darauf hinweisen, dass die Wahlmöglichkeit (hierzu sogleich) bei mehreren Rechtsgrundlagen durch die verschiedenen Anwendungsbereiche beschränkt ist.

<sup>45</sup> Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 10; Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 24; *Krusche*, ZD 2020, S. 232, 233; *Veil*, NJW 2018, S. 3337, 3338; Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 5; *Kübling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 371; Jähnel/*Jähnel*, DSGVO, 2021, Art. 6 DS-GVO, Rn. 6; Ulmer-Eilfort/*Obergfell/Herbort*, Verlagsrecht, 2. Aufl. 2021, 1. Kapitel, I., Rn. 1075.

Stellung zu, die den Verantwortlichen dazu zwingt, vorrangig die Datenverarbeitung auf die Einwilligung zu stützen.<sup>46</sup> Vielmehr stehen nach herrschender Ansicht die Rechtsgrundlagen gleichberechtigt nebeneinander.<sup>47</sup>

Eine bestimmte Beschränkung wird allenfalls bei einem Wechsel der Rechtsgrundlagen, vor allem von der Einwilligung zu einem der gesetzlichen Rechtsgrundlagen, diskutiert. Dabei geht es um die Frage, ob der Verantwortliche, der sich einmal für die Rechtsgrundlage der Einwilligung entschieden hat, bei einer Verweigerung der Einwilligung oder bei einem Widerruf auf eine gesetzliche Rechtsgrundlage wechseln kann.<sup>48</sup> Diese Konstellation hat für die hier betrachteten Fälle allerdings keine Bedeutung. Denn zum einen besteht das Problem bei

---

<sup>46</sup> Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 10; Krusche, ZD 2020, S. 232, 233; Veil, NJW 2018, S. 3337, 3338, spricht insofern von einem „Wahlrecht“; ähnlich Kollmar/El-Auwad, K&R 2021, S. 73, 77; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 25; Drewes, CR 2016, S. 721, 723; Härting/Gössling/Dimov, ITRB 2017, S. 169, 170; Jahnel/Jahnel, DSGVO, 2021, Art. 6 DS-GVO, Rn. 6; vgl. Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 11; grds wohl auch Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 10, siehe aber auch Rn. 26, wo es für Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO den Anschein hat, dass ein solches Stufenverhältnis zugrunde gelegt wird. Dieses könnte sich allerdings auch rein faktisch ergeben, wenn aus Gründen der Rechtssicherheit vorrangig die spezifischeren Tatbestände in Betracht gezogen werden. Siehe hierzu auch die Ausführungen unter: Kap. 8, C., III., 2., c) *Abwägende Rechtsgrundlage*.

<sup>47</sup> Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 10; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 2; Kuner/Bygrave/Docksey/Kotschy, GDPR, 2020, p. 329; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 14; Veil, NJW 2018, S. 3337, 3338; Krusche, ZD 2020, S. 232, 233; Kollmar/El-Auwad, K&R 2021, S. 73, 77; Drewes, CR 2016, S. 721, 723; Feiler/Forgó, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 6 DS-GVO, Rn. 2; differenzierter BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 24, 27 f., die die Rechtsgrundlagen zwar grundsätzlich gleichberechtigt nebeneinander sehen, sich im konkreten Fall aber auch ein Rangverhältnis ergeben kann. Siehe auch Klaas, CCZ 2020, S. 256, 261, der jedoch hinsichtlich der Art. 6 Abs. 1 UAbs. 1 lit. b)-e) DS-GVO eine „auf das jeweilige Interesse beschränkende Spezialität“ im Verhältnis zu Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO sieht.

<sup>48</sup> Siehe zu dieser Diskussion allgemein: Plath/Plath/Struck, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 7 f.; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 47 ff.; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 23; Härting/Gössling/Dimov, ITRB 2017, S. 169, 171; Freund u.a./Schmidt, DSGVO, 2023, Art. 6 DS-GVO, Rn. 31 ff. Siehe in diesem Kontext zur

einem Wechsel der Rechtsgrundlage und nicht wie hier, in der Anwendbarkeit und ersten Auswahl einer Rechtsgrundlage. Zum anderen dürfte, wie sogleich noch zu zeigen ist, der Einwilligung hier grds. nur eine nachrangige Bedeutung zukommen. Der Streit bedarf daher hier keinem Ergebnis.

## II. Schlussfolgerungen und denkbare Rechtsgrundlagen für datenverarbeitende TOM

Nach der Datenschutz-Grundverordnung ist es nicht ausgeschlossen, dass eine Datenverarbeitung unter mehrere Rechtsgrundlagen subsumiert werden kann, wovon am Ende mindestens eine Rechtsgrundlage bestehen muss, damit die Daten rechtmäßig verarbeitet werden dürfen. Weiterhin liegt den Rechtsgrundlagen auch keine besondere Rangfolge zugrunde, nach der der Verantwortliche gezwungen wäre, zunächst bestimmte Rechtsgrundlagen vor- oder nachrangig zu behandeln. Die Rechtsgrundlagen nach Art. 6 Abs. 1 DS-GVO stehen daher gleichberechtigt nebeneinander. Sind demnach mehrere Rechtsgrundlagen einschlägig, hat der Verantwortliche ein Wahlrecht.<sup>49</sup>

Für das Problem datenverarbeitender TOM kommt es damit im Ergebnis nicht darauf an, welche Rechtsgrundlage die Basis für die Verarbeitung bildet. Zwar können bestimmte Rechtsgrundlagen aufgrund ihrer jeweiligen Modalitäten für einzelne datenverarbeitende TOM besser geeignet sein als andere. Die Wahl einer „besseren“ Rechtsgrundlage kann und muss dann aber anhand der jeweiligen Verarbeitung und damit nach den jeweiligen TOM getroffen werden. Nicht nur, weil die Arbeit keine Untersuchung auf der Ebene einzelner datenverarbeitender TOM anstrebt,<sup>50</sup> ist eine Fixierung auf eine bestimmte Rechtsgrundlage hier weder erforderlich noch zu empfehlen. Denn ein pauschaler Fokus auf eine geeignete aber im Einzelfall vielleicht nicht „beste“ Rechtsgrundlage

---

wichtigen Differenzierung zwischen dem Wechsel einer Rechtsgrundlage beim Wegfall der ursprünglichen Rechtsgrundlage und dem Wegfall einer Rechtsgrundlage bei Kumulation: *Krusche*, ZD 2020, S. 232, 234 f., 236.

<sup>49</sup> *Veil*, NJW 2018, S. 3337, 3338; ähnlich *Kollmar/El-Auwad*, K&R 2021, S. 73, 77; *Kühling/Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 22.

<sup>50</sup> Siehe hierzu: Kap. 3, C., I. *Betrachtung des Gesamtproblems*.

könnte den Blick frühzeitig zu stark einschränken und zu einer Pfadabhängigkeit<sup>51</sup> führen, wodurch besseren Alternativen dann vielleicht keine Beachtung mehr geschenkt wird.

Möchte man dennoch bereits frühzeitig mögliche Rechtsgrundlagen für datenverarbeitende TOM evaluieren, könnte die Verarbeitung aufgrund eines berechtigten Interesses nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO eine denkbare Rechtsgrundlage darstellen.<sup>52</sup> Der Anwendungsbereich dieser Rechtsgrundlage wird grds. als sehr flexibel angesehen.<sup>53</sup> Zudem nennt die Datenschutz-Grundverordnung als Beispiel eines solchen berechtigten Interesses in ErwG 49 DS-

<sup>51</sup> Siehe grundlegend zur Pfadabhängigkeit: *David*, AER Vol. 75 (1985), pp. 332 ff., am Beispiel der Durchsetzung der "QWERTY"-Tastatur; *Arthur*, The Economic Journal Vol. 99 (1989), pp. 116 ff., am Beispiel der Durchsetzung von Technologien; *Barnes/Gartland/Stack*, JEI Vol. 38 (2004), pp. 371 ff., mit Fokus auf „Behavioral Lock-In“. Siehe auch Arthur [Ed.], *Increasing returns and path dependence in the economy*, 1994. Für einen allgemeinen Überblick: *Staatslexikon/Beyer*, 4. Bd., 8. Aufl. 2020, S. 761 ff., Begriff: „Pfadabhängigkeit“.

<sup>52</sup> Auf diese Rechtsgrundlage verweisen in dem Kontext von Art. 32 DS-GVO: *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 43 f.; *Wybitul/Schreiberbauer/Spittka*, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 32 DS-GVO, Rn. 22; *Kipker/Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 43; *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 27; *Hören/Sieber/Holznapel/Schmitz*, Hdb. Multimedia-Recht, Stand: 59. EL. 2023, Teil 16.2, Rn. 359 f. (Stand: Oktober 2020), wobei auch eine Anknüpfung an Art. 6 Abs. 1 UAbs. 1 lit. b) und c) DS-GVO denkbar sei; *Joos/Nägele*, DuD 2022, S. 578, 581 f., am Fall von Softwaretestungen mit personenbezogenen Daten; *Poncza*, ZD 2023, S. 8, 10, am Fall von „Penetration Tests“, verweist aber auf das Problem einer „kritischen Einzelfallprüfung“; *Taeger/Pohle/Deutsch/Eggendorfer*, Computerrechts-Hdb., Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 328 (Stand: Mai 2022), mit allgemeinem Verweis auf Maßnahmen der IT-Sicherheit; siehe auch *Freund u.a./Schmidt*, DSGVO, 2023, Art. 6 DS-GVO, Rn. 50, mit dem Hinweis, dass diese Rechtsgrundlage nur für „normale personenbezogene Daten“ zur Verfügung stünde und sieht daher wohl eher die Rechtsgrundlage der „primären Datenverarbeitung“ hierfür geeignet (siehe hierzu bereits: Kap. 9, B., II. *Anforderungen an den Zweck der Verarbeitung*, Fn. 36). A.A. *Hornung/Schallbruch/Jandt*, IT-Sicherheitsrecht, 2021, § 17, Rn. 58, die die Anwendbarkeit dieser Rechtsgrundlage für Maßnahmen des Art. 32 DS-GVO ablehnt, da diese gesetzlich verpflichtet seien; ähnlich wohl auch *Jandt/Steidle/Steidle*, Datenschutz im Internet, 2018, B., III., Rn. 306 ff., der aufgrund der bestehenden Pflichten den Anwendungsbereich des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO im Lichte des ErwG 49 DS-GVO für unklar hält.

<sup>53</sup> *Gierschmann u.a./Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 119; *Kühling/Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 141; *Simitis/Hornung/Spiecker* gen. *Döhmann/Schantz*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 86; *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn.

GVO ausdrücklich die Netz- und Informationssicherheit.<sup>54</sup> Aus den Erklärungen des Erwägungsgrunds lassen sich dabei Schnittmengen mit der Sicherheit der Verarbeitung i.S.d. Art. 32 DS-GVO ableiten, die durch datenverarbeitende TOM adressiert werden könnten.<sup>55</sup>

### III. Die Untauglichkeit der Einwilligung

Das bedeutet aber nicht, dass die „Auswahl“ einer passenden Rechtsgrundlage für datenverarbeitende TOM überhaupt keine Bedeutung hat. Denn eine Besonderheit bei der „Wahl“ einer passenden Rechtsgrundlage könnte die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO betreffen.

#### 1. Rechtsunsicherheit über die Zustimmung

Wie bereits ausgeführt, kann die Einwilligung gem. Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO der betroffenen Person eine Datenverarbeitung rechtfertigen. Der Gesetzgeber stellt dabei grds. keine inhaltlichen Anforderungen an die Einwilli-

---

411; *Herfurth*, ZD 2018, S. 514, 514; *Plath/Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 58, „tendenziell sehr weiten Erlaubnistatbestand“.

<sup>54</sup> *Spindler/Schuster/Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 15; *Kühling/Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 167; *Taeger/Gabel/Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 138; *Simitis/Hornung/Spiecker* gen. *Döhmman/Schantz*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 119; *Gola/Heckmann/Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 64 „von Gesetzes wegen berechtigt“.

<sup>55</sup> Auf ErwG 49 im Zusammenhang des Art. 32 DS-GVO verweisen auch *v. Lewinski/Rüpkke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 44; ähnlich *Kipker/Reusch/Ritter/Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 71, im Kontext des Art. 32 Abs. 4 DS-GVO, die aber wohl ErwG 49 S. 1 DS-GVO nicht auf den gesamten Anwendungsbereich des Art. 32 DS-GVO erstrecken und sonst die Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. c) i.V.m. Art. 32 DS-GVO stützen wollen; siehe auch im Zusammenhang des Art. 32 Abs. 4 DS-GVO *Wybitul/Schreiberbauer/Spittka*, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 32 DS-GVO, Rn. 22, die auf ErwG 49 und Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO verweisen; ähnlich *Spindler/Schuster/Laue*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 32 DS-GVO, Rn. 27. Wohl allgemein zu Maßnahmen der Informationssicherheit *Kipker/Voskamp/Klein*, Cybersecurity, 2. Aufl. 2023, Kapitel 7, Rn. 43; *Sassenberg/Faber/Mantz/Spittka*, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 176, allgemein zu Maßnahmen der IT-Sicherheit.

gung in der Form, dass betroffene Personen nur in bestimmte Verarbeitungszwecke einwilligen können.<sup>56</sup> Die gesetzlichen Vorgaben an die Einwilligung beschränken sich vielmehr darauf sicherzustellen, dass die Einwilligung das ausdrückt, was sie als Rechtsgrundlage für eine Datenverarbeitung legitimiert – eine selbstbestimmte Entscheidung der betroffenen Person zugunsten der Datenverarbeitung.<sup>57</sup> Die Einwilligung ist grds. eine sehr umfangreiche Rechtsgrundlage, mit einem sehr weiten Anwendungsgebiet für eine Vielzahl verschiedener Verarbeitungen.<sup>58</sup>

Damit käme die Einwilligung auch grds. für die Verarbeitung im Rahmen datenverarbeitender TOM in Betracht. Dennoch eignet sie sich primär nicht als Rechtsgrundlage für die hier in Frage stehenden datenverarbeitenden TOM. Der Grund dafür liegt in der Kehrseite des Legitimationsgedanken der Einwilligung, der sie zu dieser potentiell umfassenden Rechtsgrundlage macht. Denn datenverarbeitende TOM sollen die gesetzlichen Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO gewährleisten. Können einzelne TOM nicht implementiert werden, kann dies dazu führen, dass die Anforderungen nach Art. 32 DS-GVO nicht erfüllt sind. Verantwortliche brauchen daher ein ausreichendes Maß an Rechtssicherheit.

Die Einwilligung und damit die Rechtmäßigkeit der Verarbeitung hängt von der Zustimmung der betroffenen Person ab, vgl. Art. 4 Nr. 11 DS-GVO. Um nicht zu riskieren, dass die betroffene Person die Einwilligung verweigert und damit die Pflicht zur Gewährleistung der Sicherheit der Verarbeitung gefährdet, liegt es bereits grundlegend nicht im Interesse des Verantwortlichen diese Frage überhaupt von der Entscheidung der betroffenen Person abhängig zu machen.

---

<sup>56</sup> Siehe hierzu bereits: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen.*

<sup>57</sup> Siehe hierzu bereits: Kap. 8, C., II. *Die Selbstbestimmung der betroffenen Person als Legitimation.*

<sup>58</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 3; siehe ebenfalls die Einordnung als „Schlüssel zu einem unbegrenzten Datenzugang“, allerdings in der Gesamtbetrachtung auch kritisch: Kollmar/El-Auwad, K&R 2021, S. 73, 73; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 24; Plath/Plath/Struck, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 9.

## 2. Widerrufsrecht

Die Rechtsunsicherheit, die die Einwilligung mit sich bringt, wird noch verstärkt durch das Widerrufsrecht, das der betroffenen Person zusteht. Denn die betroffene Person hat nicht nur die Möglichkeit die Einwilligung zu verweigern und damit die Rechtmäßigkeit der Verarbeitung gleich von Beginn an zu verhindern. Gem. Art. 7 Abs. 3 DS-GVO kann die betroffene Person, nachdem sie die Einwilligung erklärt hat, diese auch jederzeit und ohne Angaben von Gründen widerrufen.<sup>59</sup> Zwar bleibt die Verarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig.<sup>60</sup> Der Widerruf hat aber zur Folge, dass die Datenverarbeitung ab dem Zeitpunkt des Widerrufs nicht länger vorgenommen werden darf und wirkt damit ex nunc.<sup>61</sup>

---

<sup>59</sup> Ehmman/Selmayr/Heckmann/Paschke, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 86; Schwartmann u.a./Klein/Schwartmann, DS-GVO/BDSG, 2. Aufl. 2020, Art. 7 DS-GVO, Rn. 39; Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 46; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 7 DS-GVO, Rn. 16; Gierschmann u.a./Gierschmann, Datenschutz-Grundverordnung, 2018, Art. 7 DS-GVO, Rn. 119; Wächter, Datenschutz im Unternehmen, 6. Aufl. 2021, Rn. 306; Knyrim/Wyrobek, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 6.46; Ernst, ZD 2020, S. 383, 384; Jahnel/Pallwein-Prettner, Datenschutzrecht, 3. Aufl. 2021, S. 75; Wybitul/Fladung/Pötters, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 7, 8 DS-GVO, Rn. 23.

<sup>60</sup> Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 7 DS-GVO, Rn. 79; Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 48; Dat-Komm/Kastelitz, Stand: 76. EL. 2023, Art. 7 DS-GVO (Stand: Juli 2020), Rn. 28, 32; Spiecker gen. Döhmann u.a./Raubofer/Schafer, GDPR, 2023, Art. 7 GDPR, Rn. 36; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 7 DS-GVO, Rn. 11; Gierschmann u.a./Gierschmann, Datenschutz-Grundverordnung, 2018, Art. 7 DS-GVO, Rn. 120; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 7 DS-GVO, Rn. 16; Ernst, ZD 2020, S. 383, 384; Jahnel/Pallwein-Prettner, Datenschutzrecht, 3. Aufl. 2021, S. 75; Wybitul/Fladung/Pötters, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 7, 8 DS-GVO, Rn. 24; vgl. Auernhammer/Kramer, 8. Aufl. 2024, Art. 7 DS-GVO, Rn. 35.

<sup>61</sup> Plath/Plath, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 7 DS-GVO, Rn. 15; Schwartmann u.a./Klein/Schwartmann, DS-GVO/BDSG, 2. Aufl. 2020, Art. 7 DS-GVO, Rn. 40; Dat-Komm/Kastelitz, Stand: 76. EL. 2023, Art. 7 DS-GVO (Stand: Juli 2020), Rn. 32; Ernst, ZD 2020, S. 383, 384; Kübling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 529; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 7 DS-GVO, Rn. 79; Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 46; Spindler/Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 7 DS-GVO, Rn. 11; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 7 DS-GVO, Rn. 16; Spiecker gen. Döhmann u.a./Raubofer/Schafer, GDPR, 2023, Art. 7 GDPR, Rn. 36.

Art. 7 Abs. 3 DS-GVO stellt dabei keine nennenswerten Anforderungen an die Ausübung des Widerrufsrechts.<sup>62</sup> Auch ein Ausschluss oder eine Einschränkung des Widerrufs für bestimmte Situationen lassen sich aus Art. 7 Abs. 3 DS-GVO nicht ableiten.<sup>63</sup> Ferner dürfte auch ein Verzicht der betroffenen Person auf die Ausübung ihres Widerrufsrechts nicht ohne weiteres möglich sein.<sup>64</sup>

Die Unsicherheit über die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung besteht daher nicht nur im Zeitpunkt der erstmaligen Erteilung der Einwilligung, sondern erstreckt sich über den gesamten Verarbeitungszyklus. Aufgrund des Widerrufsrechts muss der Verantwortliche jederzeit damit rechnen, dass die einmal wirksam erteilte Einwilligung widerrufen und damit die Rechtsgrundlage für die Verarbeitung nachträglich entzogen wird.

---

<sup>62</sup> Ehmman/Selmayr/Heckmann/Paschke, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 91; Gola/Heckmann/Schultz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 54; Veil, NJW 2018, S. 3337, 3341.

<sup>63</sup> Kühling/Buchner/Buchner/Kühling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 39; Schantz/Wolff/Schantz, Das neue Datenschutzrecht, 2017, Rn. 532; Jahnelt/Pallwein-Prettner, Datenschutzrecht, 3. Aufl. 2021, S. 75; grds. wohl auch Auernhammer/Kramer, 8. Aufl. 2024, Art. 7 DS-GVO, Rn. 34, siehe jedoch die nachfolgenden Ausführungen. Diskutiert wird ein Ausschluss oder eine Einschränkung des Widerrufs, wenn die Einwilligung Gegenstand eines Vertrages ist: Moos/Schefzig/Arning/Rohwedder, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 285, ohne abschließende Stellungnahme; Simitis/Hornung/Spiecker gen. Döhmman/Klement, Datenschutzrecht, 2019, Art. 7 DS-GVO, Rn. 92; Kühling/Buchner/Buchner/Kühling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 38 ff., im Ergebnis aber ablehnend (Rn. 39), wobei die Berücksichtigung der vertraglichen Interessen erreicht wird, indem die Verarbeitung neben der Einwilligung auf Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO gestützt werden soll (Rn. 39b); für eine Einschränkung Ernst, ZD 2020, S. 383, 384 f., im Wege einer teleologischen Reduktion des Art. 7 Abs. 3 DS-GVO; Auernhammer/Kramer, 8. Aufl. 2024, Art. 7 DS-GVO, Rn. 34, aber ohne methodische Begründung; Krohm, ZD 2016, S. 368, 373, will die Ausübung des Widerrufs in Vertragsverhältnissen (auch unter der Datenschutz-Grundverordnung) am „Grundsatz von Treu und Glauben“ ausrichten.

<sup>64</sup> Sydow/Marsch/Ingold, DS-GVO – BDSG, 3. Aufl. 2022, Art. 7 DS-GVO, Rn. 46; Auernhammer/Kramer, 8. Aufl. 2024, Art. 7 DS-GVO, Rn. 34; Jahnelt/Jahnelt, DSGVO, 2021, Art. 7 DS-GVO, Rn. 17, mit Verweis auf eine Entscheidung der österreichischen Datenschutzbehörde (DSB, DSB-D213.692/0001-DSB/2018, Rn. 3.2.3.); vgl. Kühling/Buchner/Buchner/Kühling, DS-GVO – BDSG, 4. Aufl. 2024, Art. 7 DS-GVO, Rn. 35, die jedenfalls einen „endgültig[en] und abschließend[en]“ Verzicht ablehnen; ähnlich Spiecker gen. Döhmman u.a./Raubofer/Schafer, GDPR, 2023, Art. 7 GDPR, Rn. 35, die aber die Möglichkeit einer Modifikation, wie einer Frist, für möglich halten; Ernst, ZD 2020, S. 383, 384, hält einen Verzicht individualvertraglich wohl für denkbar.



Aus Planungssicht dürfte das Widerrufsrecht für den Verantwortlichen sogar gravierender sein als die Möglichkeit der Verweigerung der betroffenen Person, in die Verarbeitung einzuwilligen. Denn in diesem Fall laufen bereits die Pflichten nach Art. 32 DS-GVO und der Verantwortliche müsste kurzfristig einen Ersatz für die Maßnahmen finden, die durch den Widerruf der betroffenen Personen wegfallen.

### 3. Berücksichtigung im Rahmen des Art. 32 DS-GVO?

Fraglich ist, ob sich die Unsicherheiten mit der Einwilligung nicht in Art. 32 DS-GVO berücksichtigen lassen.

#### a) Verweigerung oder Widerruf der Einwilligung als Verzicht auf den Schutz nach Art. 32 DS-GVO

So könnte man überlegen, ob die Verweigerung der Einwilligung in die Verarbeitung datenverarbeitender TOM oder deren Widerruf gleichzeitig als Verzicht auf den Schutz nach Art. 32 DS-GVO anzusehen ist. Ob ein solcher Verzicht überhaupt möglich ist, ist derzeit noch stark umstritten.<sup>65</sup> Doch selbst wenn man die Möglichkeit eines solchen Verzichts annähme, bleibt die Anwendung auf die hier relevanten Fälle in zweierlei Hinsicht fraglich.

Möchte man die Verweigerung oder den Widerruf der Einwilligung in die Datenverarbeitung der TOM gleichzeitig als Verzicht auf den Schutz nach Art. 32 DS-GVO deuten, so könnte dies nur bei Personengleichheit gelten. Die Person muss gleichzeitig von der Datenverarbeitung der TOM als auch von der

---

<sup>65</sup> Siehe allgemein zu der Frage nach einem „Verzicht“ auf bzw. einer „Disponibilität“ von Art. 32 DS-GVO weiterführend insbesondere: *Franck*, CR 2016, S. 238 ff.; *Sundermann*, DuD 2021, S. 594 ff.; *John/Schaller*, CR 2022, S. 156 ff.; *Laue/Kremer/Laue*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 7, Rn. 29; *Plath/Grages*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 2; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 39 f.; *Gola/Heckmann/Piltz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 44; *Schwartzmann u.a./Ritter*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 20; *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 4a ff.; *Bleckat*, RDV 2021, S. 206 ff.; *v. Lewinski/Rüpkke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 9a; *Eusani*, DS 2019, S. 18, 26. Siehe auch *Lotz/Wendler*, CR 2016, S. 31 ff., die diese Frage zwar anhand von § 9 BDSG a.F. erörtern, in einem Ausblick aber noch kurz auf die Rechtslage nach den Entwürfen der Datenschutz-Grundverordnung eingehen.

nach Art. 32 DS-GVO zu schützenden Datenverarbeitung betroffen sein. Andernfalls könnte in der Verweigerung oder des Widerrufs der Einwilligung gleichzeitig keine Aussage zu Art. 32 DS-GVO gesehen werden. Diese Personengleichheit ist allerdings nicht zwingend und wohl auch nicht der überwiegende Anwendungsbereich.

Doch auch aus der Perspektive des Art. 6 DS-GVO gäbe es Zweifel an einer solchen Interpretation. Würde man die Verweigerung oder den Widerruf der Einwilligung gleichzeitig als Verzicht auf den rechtlichen Schutz ansehen, stellt sich bereits die Frage, ob sich die betroffene Person dann überhaupt in der Ausgangslage befunden hat, eine freie Entscheidung über die Datenverarbeitung zu treffen, die aber zwingende Voraussetzung einer Einwilligung ist (vgl. Art. 4 Nr. 11 DS-GVO). Hieran wäre jedenfalls zu zweifeln, wenn die betroffene Person damit vor die „Wahl“ gestellt wird, entweder der Datenverarbeitung zuzustimmen oder – in Konsequenz ihrer Verweigerung oder eines nachträglichen Widerrufs – auf den Mindestschutz nach Art. 32 DS-GVO zu verzichten. Vor eine solche Wahl dürfte die betroffene Person nach den Grundsätzen der Einwilligung wohl nicht gestellt werden.<sup>66</sup>

### *b) Allgemeine Berücksichtigung im Rahmen der Angemessenheitsprüfung*

Unabhängig davon, ob eine Personengleichheit hinsichtlich der datenverarbeitenden TOM und der zu schützenden Verarbeitung betroffenen Personen bestünde, könnte man allgemein versuchen die Verweigerung oder den Widerruf

---

<sup>66</sup> Siehe allgemein zu dem Problem, dass der betroffenen Person ein niedrigeres Schutzniveau aufgezwungen werden könnte: *Sundermann*, DuD 2021, S. 594, 595, 597. An dieser Stelle ist jedoch darauf hinzuweisen, dass im Rahmen der Diskussion über den Verzicht auf ein (bestimmtes) Schutzniveau nach Art. 32 DS-GVO (siehe hierzu ausführlicher die Nachweise in Fn. 65) häufig das Instrument der Einwilligung i.S.d. der Datenschutz-Grundverordnung genannt wird. Das hierin die (einzige) Möglichkeit des Verzichts liegt, wird hier nicht vertreten. Es könnte auch ein allgemeiner Rechtsverzicht (bei dem aber Parallelen zur Definition der Einwilligung i.S.d. Art. 4 Nr. 11 DS-GVO bestehen dürften) in Betracht kommen. Das Problem muss hier nicht weiter geklärt werden. Es soll nur darauf hingewiesen werden, dass hier im Rahmen einer datenschutzrechtlichen Einwilligung über eine datenverarbeitende TOM bzw. besser deren Verweigerung oder Widerruf gleichzeitig eine Aussage über einen möglichen Verzicht auf den Schutz nach Art. 32 DS-GVO gesehen werden könnte, was dann allerdings Einfluss auf die Einwilligung über die TOM hätte. Dagegen soll hier keine Stellung zu der Frage bezogen werden, ob man in einen niedrigeren Schutz nach Art. 32 DS-GVO mit einer *datenschutzrechtlichen Einwilligung* einwilligen kann.

der Einwilligung innerhalb des Pflichtenumfangs des Art. 32 DS-GVO zu berücksichtigen. In dieser Arbeit wird gerade vertreten, dass im Rahmen der Angemessenheitsprüfung nach Art. 32 DS-GVO die datenschutzrechtliche Rechtmäßigkeit der TOM berücksichtigt werden sollte.<sup>67</sup> Dies kann allerdings nicht dahingehend interpretiert werden, dass sich hiermit die Rechtsunsicherheiten der Einwilligung ausgleichen lassen sollten.

Eine datenverarbeitende TOM ist dann unzulässig und kann dementsprechend im Rahmen des Art. 32 DS-GVO berücksichtigt werden, wenn keine Rechtsgrundlage eingreift. Es wäre daher nicht ausreichend, wenn nur die Einwilligung verweigert oder widerrufen würde. Dazu dürfte dann auch keine gesetzliche Rechtsgrundlage die Datenverarbeitung legitimieren können. Sofern aber eine gesetzliche Rechtsgrundlage besteht, ist ein Rückgriff auf die Einwilligung aufgrund der genannten Rechtsunsicherheit aber ohnehin nicht zu empfehlen.

Problematisch wären dann nur noch die Fälle, in denen keine gesetzliche Rechtsgrundlage einschlägig ist und die letzte Möglichkeit für eine rechtmäßige Datenverarbeitung in der Einwilligung läge. Doch gerade in diesen Fällen dürften dann die Voraussetzungen einer wirksamen Einwilligung entgegenstehen. Würde man den Verantwortlichen im Rahmen des Art. 32 DS-GVO dafür verantwortlich machen, dass er nicht versucht hat eine Einwilligung in die Datenverarbeitung der datenverarbeitenden TOM von der betroffenen Person zu erhalten, dann wird der Verantwortliche alles unternehmen, um diese Einwilligung zu bekommen. Dadurch steigt aber der Druck auf die betroffene Person in die Verarbeitung einzuwilligen. Eine Fremdbestimmung ist hier schon praktisch vorprogrammiert. In einer solchen Situation kann die betroffene Person nicht wirksam einwilligen.

### *c) Praktische Probleme*

Abschließend verdient noch ein eher praktisches Argument Beachtung, das im Zusammenhang des allgemeinen Verzichts auf den Schutz nach Art. 32 DS-GVO angeführt wird. Die Sicherheit der Verarbeitung wird in der Regel für den

---

<sup>67</sup> Siehe hierzu ausführlicher: Kap. 7 *Berücksichtigung datenverarbeitender TOM*.

gesamten Verarbeitungsprozess konzipiert.<sup>68</sup> Bspw. wird ein Server durch entsprechende Maßnahmen insgesamt vor unbefugten Zugriffen geschützt. Gleichzeitig sind sowohl innerhalb der zu schützenden Verarbeitung aber auch durch die Verarbeitung im Rahmen der TOM meist mehrere Personen betroffen.

Es ist für den Verantwortlichen hier kaum möglich, anhand der Zustimmungen oder auch Verweigerungen der Einwilligung durch den einzelnen Betroffenen eine entsprechende Sicherheitsstruktur aufzubauen, die diese Individualitäten berücksichtigen kann.<sup>69</sup> Ziel des Verantwortlichen ist es, eine ganzheitliche Sicherheit für die Modalitäten der jeweiligen Verarbeitung – als Zusammenfassung aller identischen Einzelverarbeitungen – zu gewährleisten.

Aus dieser faktischen Erwägung heraus, kann der Verantwortliche das Sicherheitsniveau nicht für jede einzelne betroffene Person, aus der Gruppe einer Verarbeitung, anpassen. Damit bedarf es auch für datenverarbeitende TOM einer Rechtsgrundlage, die nicht auf die Individualitäten wie der Zustimmung einzelner Personen abstellt, sondern an den Gegebenheiten der gesamten, zu schützenden Verarbeitung ausgerichtet sind.

#### 4. Denkbare Anwendungsfälle und Zwischenergebnis

Der Nachteil der Rechtsunsicherheit, den die Einwilligung mit sich bringt, kann der Verantwortliche im Rahmen datenverarbeitender TOM grundsätzlich nicht in Kauf nehmen. Ein Rückgriff auf die Einwilligung wäre allenfalls in den Fällen denkbar, in denen der Verantwortliche mit den jeweiligen datenverarbeitenden TOM gezielt über die Mindestanforderungen nach Art. 32 DS-GVO hinausgehen möchte. Dies kann gerade für Verantwortliche interessant sein, die

---

<sup>68</sup> Vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 40; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 20; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 4c. Siehe allgemein im Rahmen der Netz- und Informationssicherheit Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 59.

<sup>69</sup> Vgl. Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 20; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 40; Plath/Grages, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 2; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 4c. Siehe auch zum Problem der Einwilligung als Rechtsgrundlage im Kontext der Erfassung von Zugriffen allgemein im Rahmen der Netz- und Informationssicherheit Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 59.

versuchen möchten, mit einem hohen Sicherheitsniveau eine Vertrauensposition auf dem Markt zu erlangen, um Kunden zu gewinnen.<sup>70</sup> Ein Beispiel hierfür könnte die (freiwillige) Einrichtung eines Fingerabdruckscanners anstelle einer Passworteingabe als Authentifizierungssystem oder die Einrichtung einer (zusätzlichen) 2-Faktor-Authentifizierung darstellen.

Verlässt der Verantwortliche den Pflichtbereich des Art. 32 DS-GVO, muss er nicht fürchten, dass eine Verweigerung der Einwilligung oder ihr nachträglicher Widerruf Auswirkungen auf die Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DS-GVO hat. Damit reduzieren sich denkbare Anwendungsfälle für eine Einwilligung bereits deutlich. Ergänzend sollte man hier auch berücksichtigen, dass ein solcher Rückgriff auf die Einwilligung wohl wieder die Personengleichheit voraussetzt und es sich sowohl bei der, nach Art. 32 DS-GVO zu schützenden betroffenen Person als auch bei der, durch die datenverarbeitenden TOM betroffenen Person um dieselbe Person handeln muss. Damit reduziert sich der denkbare Anwendungsfall noch weiter.

Da es sich hierbei allerdings um einen sehr kleinen Ausnahmereich handelt, der zudem den hier untersuchten Pflichtenbereich des Art. 32 DS-GVO verlässt, kann der Nachteil der Rechtsunsicherheit, den die Einwilligung zwangsweise mit sich bringt, in den hier relevanten Konstellationen, nicht ausgeglichen werden. Trotz ihres grds. weiten Anwendungsbereichs ist sie damit als Rechtsgrundlage für die hier relevanten Fälle nicht geeignet.<sup>71</sup>

---

<sup>70</sup> Siehe zuvor kurz zur Sicherheit der Verarbeitung als möglicher Wettbewerbsvorteil: Kap. 3, C., II. *Beschränkung auf den unternehmerischen Bereich*, insb. Fn. 3.

<sup>71</sup> Siehe auch die Einschätzungen von: Kipker/*Voskamp/Klein*, *Cybersecurity*, 2. Aufl. 2023, Kapitel 7, Rn. 42e, allgemein zu Maßnahmen der Datensicherheit und besonders auf die Widerrufbarkeit gestützt; Taeger/Pohle/*Deusch/Eggendorfer*, *Computerrechts-Hdb.*, Stand: 38. EL. 2023, Teil 5, 50.1 IT-Sicherheit, Rn. 330 (Stand: Mai 2022), zu Maßnahmen der IT-Sicherheit unter Verweis auf den Widerruf und den Besonderheiten der Freiwilligkeit im Beschäftigungsverhältnis; Hornung/Schallbruch/*Jandt*, *IT-Sicherheitsrecht*, 2021, § 17, Rn. 59, allgemein zur Netz- und Informationssicherheit; Joos/*Nägele*, *DuD* 2022, S. 578, 581, zum Fall von Softwaretestungen mit personenbezogenen Daten; ähnlich *Poncza*, *ZD* 2023, S. 8, 10, der im Fall von „*Penetration Tests*“ die verfolgten Ziele gefährdet sieht; ähnlich auch *Schlegel*, *ZD* 2020, S. 243, 244 für „*Data-Loss-Prevention-Software*“, mit Verweis auf die Möglichkeit des jederzeitigen Widerrufs, aber auch mit Bedenken hinsichtlich der Freiwilligkeit; siehe zum Einsatz von „*Angriffserkennungssystemen*“ *Krügel*, *MMR* 2017, S. 795, 798; ähnlich *Deusch/Eggendorfer*, *Intrusion Detection und DSGVO*, in: *Rechtsfragen digitaler Transformationen*, 2018, S. 741, 748, zum Einsatz von „*Intrusion Detection*“ Systemen; *Schulte/Wambach*, *DuD* 2020, S. 462, 465, zum Fall von „*Log-files*“ zur späteren Aufklärung von IT-Sicherheitsverletzungen.

#### IV. Das Widerspruchsrecht als Ausschlussgrund für gesetzliche Rechtsgrundlagen

Die Unsicherheit am Fortbestand der Rechtsgrundlage aufgrund des Widerrufs der Einwilligung stellt ein wesentliches Argument für die Ungeeignetheit der Einwilligung und damit ihren hier vertretenen Ausschluss aus der weiteren Betrachtung dar. Ähnliche Probleme wie beim Widerrufsrecht der Einwilligung könnten sich allerdings auch bei den gesetzlichen Rechtsgrundlagen ergeben.

Die Datenschutz-Grundverordnung gibt der betroffenen Person in Art. 21 DS-GVO die Möglichkeit, einer – eigentlich rechtskonformen Datenverarbeitung –<sup>72</sup> zu widersprechen. Allgemeine Folge eines erfolgreichen Widerspruchs ist, dass die Datenverarbeitung nicht länger rechtmäßig vorgenommen werden darf.<sup>73</sup> Die Verarbeitung vor Geltendmachung des Widerspruchs wird durch diesen hingegen nicht rechtswidrig.<sup>74</sup> Hinsichtlich der Möglichkeit, mit dem Widerspruch eine an sich rechtmäßige Verarbeitung für die Zukunft zu unterbinden, besteht eine Vergleichbarkeit mit dem Widerruf der Einwilligung, mit der eine wirksame Einwilligung nachträglich „angegriffen“ werden kann.<sup>75</sup>

---

<sup>72</sup> Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 21 DS-GVO, Rn. 1; *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 697; *Jahnel/Jahnel*, DSGVO, 2021, Art. 21 DS-GVO, Rn. 1; *Veil*, NJW 2018, S. 3337, 3341; *Gierschmann u.a./Veil*, Datenschutz-Grundverordnung, 2018, Art. 7 DS-GVO, Rn. 1, 12; siehe auch *Kühling/Buchner/Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 21 DS-GVO, Rn. 4, der das Widerspruchsrecht auch auf rechtswidrige Verarbeitungen anwenden möchte; ähnlich *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 21 DS-GVO, Rn. 2; *Freund u.a./Nühlen*, DSGVO, 2023, Art. 21 DS-GVO, Rn. 26, erachtet die Anwendung auf rechtswidrige Verarbeitung jedenfalls für „nicht untauglich“; wohl auch *Auernhammer/Kramer*, 8. Aufl. 2024, Art. 21 DS-GVO, Rn. 1, 18.

<sup>73</sup> *Kühling/Buchner/Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 21 DS-GVO, Rn. 2; *Jahnel/Jahnel*, DSGVO, 2021, Art. 21 DS-GVO, Rn. 1, siehe auch Rn. 26 ff. und dort insb. Rn. 27, wo darauf hingewiesen wird, dass die Folge des Widerspruchs nach Absatz 6 in der Verordnung fehlt; vgl. auch *Veil*, NJW 2018, S. 3337, 3341, der die Folgen des Widerspruchs im Gesetz für nicht so eindeutig angeordnet sieht; ähnlich *Taeger/Gabel/Munz*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 21 DS-GVO, Rn. 18 f., 41, 65, hinsichtlich des Widerspruchs nach Art. 21 Abs. 6 DS-GVO.

<sup>74</sup> *Kühling/Buchner/Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 21 DS-GVO, Rn. 2; vgl. *Auernhammer/Kramer*, 8. Aufl. 2024, Art. 21 DS-GVO, Rn. 9; *Taeger/Gabel/Munz*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 21 DS-GVO, Rn. 19, 41, 65.

<sup>75</sup> *Paal/Pauly/Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 21 DS-GVO, Rn. 2a; *Veil*, NJW 2018, S. 3337, 3341; *Kuner/Bygrave/Docksey/Zanfir-Fortuna*, GDPR, 2020, p. 516;

Art. 21 DS-GVO unterscheidet drei Fälle, in denen die betroffene Person der Verarbeitung widersprechen kann; (1) ein Widerspruchsrecht gegen Verarbeitung auf Basis bestimmter Rechtsgrundlagen (Art. 21 Abs. 1 DS-GVO), (2) ein Widerspruchsrecht gegen Verarbeitungen zum Zwecke der Direktwerbung (Art. 21 Abs. 2 und 3 DS-GVO) und ein Widerspruchsrecht gegen Verarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (Art. 21 Abs. 6 DS-GVO).<sup>76</sup> Mittels eines Widerspruchs i.S.d. Art. 21 DS-GVO können (vor allem) Verarbeitungen auf gesetzlicher Rechtsgrundlagen nachträglich unterbunden werden.<sup>77</sup>

Für die hier behandelten Fälle käme wohl einzig der Widerspruch nach Art. 21 Abs. 1 DS-GVO in Betracht, da es nicht um eine Verarbeitung für Werbezwecke (Abs. 2) oder Forschungszwecke (Abs. 6) geht. Anders als die beiden

---

siehe auch ausführlicher zum Widerruf der Einwilligung bereits oben: Kap. 9, C., III., 2. *Widerrufsrecht*.

<sup>76</sup> Kühling/Buchner/*Herbst*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 21 DS-GVO, Rn. 5; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 21 DS-GVO, Rn. 1; Spiecker gen. Döhmman u.a./*Carmichael/Cradock/Stalla-Bourdillon*, GDPR, 2023, Art. 21 GDPR, Rn. 1; Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 21 DS-GVO, Rn. 7; Jahnel/*Jahnel*, DSGVO, 2021, Art. 21 DS-GVO, Rn. 3; Ehmann/*Selmayr/Kamann/Braun*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 21 DS-GVO, Rn. 1; Sassenberg/*Faber/Mantz/Spittka*, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020, § 6, Rn. 74; Freund u.a./*Nüblen*, DSGVO, 2023, Art. 21 DS-GVO, Rn. 24; Kühling/*Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 698.

<sup>77</sup> Zwei der drei Widerspruchsrechte sind nicht speziell an eine bestimmte Rechtsgrundlage, sondern den Verarbeitungszweck gekoppelt (siehe auch zur Differenzierung der einzelnen Widerspruchsrechte: *Feiler/Forgó*, EU-DSGVO und DSGVO, 2. Aufl. 2022, Art. 21 DS-GVO, Rn. 1). Sie könnten (in der Theorie) auch für die Einwilligung genutzt werden. Da die Einwilligung inhaltlich aber das viel umfassendere Recht ist, kommt der Frage, ob auch die Einwilligung bspw. für Direktwerbung i.S.d. Art. 21 Abs. 2 DS-GVO widersprochen werden kann, faktisch keine Bedeutung zu. Siehe auch Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 21 DS-GVO, Rn. 4, der jedenfalls für den Widerspruch nach Abs. 6 auf „eine Datenverarbeitung auf jeder Rechtsgrundlage“ verweist. A.A. wohl Gola/*Heckmann/Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 21 DS-GVO, Rn. 1, der insgesamt auf gesetzliche Grundlagen abstellt; auch Freund u.a./*Nüblen*, DSGVO, 2023, Art. 21 DS-GVO, Rn. 26; ähnlich im konkreten Fall des Art. 21 Abs. 2 DS-GVO Moos/*Schefzig/Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 6, Rn. 588, der bei der Einwilligung dann einen Widerruf verlangt; siehe auch Gierschmann u.a./*Veil*, Datenschutz-Grundverordnung, 2018, Art. 7 DS-GVO, Rn. 27 f., der scheinbar für das gesamte Widerspruchsrecht nach Art. 21 DS-GVO eine Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. e) oder f) DS-GVO verlangt.

vorgenannten Widerspruchsrechte knüpft Art. 21 Abs. 1 DS-GVO nicht unmittelbar<sup>78</sup> an die Zwecke der Verarbeitung an. Das Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO bezieht sich vielmehr speziell auf die Rechtsgrundlagen nach Art. 6 Abs. 1 lit. e) und f) DS-GVO.

Anders als der Widerruf bei der Einwilligung kann die betroffene Person der Verarbeitung allerdings nicht ohne Weiteres i.S.d. Art. 21 Abs. 1 DS-GVO widersprechen.<sup>79</sup> Ein Widerspruch nach Art. 21 Abs. 1 DS-GVO ist erstmal nur möglich, wenn die betroffene Person einen besonderen Grund vorweisen kann.<sup>80</sup> Und selbst wenn ein solcher Grund vorliegt, führt dies noch nicht zwingend dazu, dass die Verarbeitung nicht länger durchgeführt werden darf. Im Fall des Art. 21 Abs. 1 DS-GVO kann der Verantwortliche dann seinerseits besondere Gründe für eine Verarbeitung anführen, die den Gründen der betroffenen Person überwiegen können und somit eine weitere Verarbeitung rechtfertigen.<sup>81</sup>

Damit lassen sich zwar grundsätzlich die gesetzlichen Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. e) und f) DS-GVO nachträglich angreifen und

---

<sup>78</sup> Durch die Beschränkung auf bestimmte Rechtsgrundlagen beschränkt sich Art. 21 Abs. 1 DS-GVO damit aber auch auf bestimmte Verarbeitungszwecke, wie auch die Beschränkung auf bestimmte Verarbeitungszwecke (vorrangig) nur bestimmte Rechtsgrundlagen trifft.

<sup>79</sup> Die Voraussetzungen des Widerspruchs im Gesamten (mit Ausnahme nach Art. 21 Abs. 2 DS-GVO) als wesentlichen Unterschied zum Widerruf stellt Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 21 DS-GVO, Rn. 2a heraus und spricht zudem von „grundsätzlich hohen Hürden“; siehe auch den Vergleich beider Rechte bei *Veil*, NJW 2018, S. 3337, 3341.

<sup>80</sup> Ehmann/Selmayr/*Kamann/Braun*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 21 DS-GVO, Rn. 19 f.; Taeger/Gabel/*Munz*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 21 DS-GVO, Rn. 14 f.; Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 21 DS-GVO, Rn. 9 f.; BeckOK Datenschutzrecht/*Forgó*, Stand: 46. Ed. 2023, Art. 21 DS-GVO (Stand: November 2021), Rn. 8; Jahnell/*Jahnell*, DSGVO, 2021, Art. 21 DS-GVO, Rn. 6; *Feiler/Forgó*, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 21 DS-GVO, Rn. 2; Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 6, Rn. 570, 572 ff.; *Veil*, NJW 2018, S. 3337, 3341; *Robrahn/Bremert*, ZD 2018, S. 291, 296; *Piltz*, K&R 2016, S. 629, 635.

<sup>81</sup> Ehmann/Selmayr/*Kamann/Braun*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 21 DS-GVO, Rn. 22 f.; Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 21 DS-GVO, Rn. 12 f.; *Veil*, NJW 2018, S. 3337, 3341; Jahnell/*Jahnell*, DSGVO, 2021, Art. 21 DS-GVO, Rn. 16; Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 6, Rn. 577, 581 ff.; Spiecker gen. Döhmann u.a./*Carmichael/Cradock/Stalla-Bourdillon*, GDPR, 2023, Art. 21 GDPR, Rn. 10; *Robrahn/Bremert*, ZD 2018, S. 291, 296; *Piltz*, K&R 2016, S. 629, 635; *Schneider*, Datenschutz, 2. Aufl. 2019, S. 204 f.



sie als Rechtsgrundlage für eine Verarbeitung entziehen. Anders als beim Widerruf der Einwilligung sind die Anwendungsfälle aufgrund der Voraussetzungen für einen solchen Widerspruch deutlich reduziert. Der Widerspruch steht damit eingriffsmäßig nicht auf einer Stufe wie der Widerruf der Einwilligung. Die Möglichkeit des Widerspruchs sollte daher kein Grund sein, die generelle Tauglichkeit einzelner, gesetzlicher Rechtsgrundlagen in Frage zu stellen.

## D. Zwischenergebnis

Vergleichbar wie der Zweckrahmen vertraglicher Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO dürfte es sich bei der Sicherheit der Verarbeitung, wie sie in Art. 32 DS-GVO dargelegt ist, eher um einen Zweckrahmen als um den konkreten Zweck der Verarbeitung handeln. So wie es bei Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO damit auf den konkreten Vertrag ankommt, müsste man die Gewährleistung der Sicherheit im Einzelfall als Zweck betrachten. Dies kann jedoch die Auswahl einer tauglichen Rechtsgrundlage für Verarbeitungen im Rahmen datenverarbeitender TOM erschweren. Denn kein Anwendungsbereich der (gesetzlichen) Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO knüpft unmittelbar an einen solchen Zweckrahmen an.

Denkbar wäre es zwar, Art. 32 DS-GVO als eine ergänzende Rechtsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) i.V.m. Abs. 3 DS-GVO einzuordnen und damit eine generelle Anknüpfung an den Zweckrahmen der Sicherheit der Verarbeitung zu erreichen. Fraglich ist, ob Art. 32 DS-GVO die Anforderungen an eine solche, ergänzende Rechtsgrundlage erfüllt. In der Verordnung gibt es deutliche Hinweise, die den Schluss zulassen, dass die Anforderungen an die ergänzende Rechtsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO hinsichtlich des ihnen zugrundeliegenden Zwecks konkreter sein müssen und einen Zweckrahmen, wie ihn Art. 32 DS-GVO wohl allenfalls enthält, nicht zulässt.

Schlussendlich können die Ergebnisse in der Frage nach der Einordnung des Art. 32 DS-GVO als ergänzende Rechtsgrundlage aber auch allgemein nach der „besten“ Rechtsgrundlage für datenverarbeitende TOM offenbleiben. Da sämtliche Rechtsgrundlagen gleichberechtigt nebeneinanderstehen und sogar mehrere Rechtsgrundlagen für eine Verarbeitung einschlägig sein können, kann später am Einzelfall entschieden werden, welche Rechtsgrundlage für die jeweilige Verarbeitung am besten geeignet ist.

Einzig zu beachten bei der Auswahl einer Rechtsgrundlage ist die Untauglichkeit der Einwilligung. Dies ergibt sich jedoch nicht aus ihrem Anwendungsbereich, denn die Einwilligung lässt grds. eine Vielzahl verschiedener Verarbeitungen zu unterschiedlichen Zwecken zu. Probleme bereitet hier, dass die Einwilligung die Zustimmung der betroffenen Person voraussetzt. Der Verantwortliche möchte mit den datenverarbeitenden TOM jedoch seine Verpflichtungen aus Art. 32 DS-GVO nachkommen. Daher kann er die Entscheidung über die Rechtmäßigkeit der Datenverarbeitung und damit auch die der datenverarbeitenden TOM nicht von der Zustimmung der betroffenen Personen abhängig machen. Eine mögliche Verweigerung der Einwilligung könnte Auswirkungen auf die Gewährleistung der Sicherheit nach Art. 32 DS-GVO und damit dessen Verpflichtungen haben, die beim Verantwortlichen zu Rechtsunsicherheiten führen, die er nicht bereit ist zu tragen. Die Rechtsunsicherheit würde zudem noch dadurch verstärkt, dass nicht nur die Abgabe der Einwilligung nicht garantiert werden kann. Ferner kann die betroffene Person ihre Einwilligung auch jederzeit widerrufen und damit diese als Rechtsgrundlage über den gesamten Verarbeitungszyklus hinweg entziehen.

Faktisch kann das Problem datenverarbeitender TOM damit nur durch eine gesetzliche Rechtsgrundlage gelöst werden. Die Suche nach einer passenden Rechtsgrundlage rückt dabei allerdings in den Hintergrund und bedarf keiner abschließenden Bewertung. Der Einzelfall kann entscheiden, welche Rechtsgrundlage für die jeweilige Verarbeitung am besten geeignet ist. Für das Problem datenverarbeitender TOM wesentlich wichtiger als die Frage nach der konkreten Rechtsgrundlage ist allerdings der weitere Tatbestand der Erforderlichkeit.

## Kapitel 10

# Der Tatbestand der Erforderlichkeit

### A. Der Tatbestand im System der Rechtsgrundlagen

Bei allen gesetzlichen Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO muss die Verarbeitung „*erforderlich*“<sup>1</sup> sein. Die gesetzlichen Rechtsgrundlagen knüpfen damit alle an den Tatbestand der Erforderlichkeit an.<sup>2</sup> Die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO kennt diese Voraussetzung hingegen

---

<sup>1</sup> Englisch: „*necessary*“, Französisch: „*nécessaire*“, Spanisch: „*necesario*“, Italienisch: „*necessario*“, Niederländisch: „*noodzakelijk*“.

<sup>2</sup> Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 9; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 9; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 15; DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 13; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 23; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 20; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 8; Ulmer-Eilfort/Obergfell/Herbort, Verlagsrecht, 2. Aufl. 2021, 1. Kapitel, I., Rn 1075.

nicht.<sup>3</sup> Die Erforderlichkeit ist somit eine Besonderheit der gesetzlichen Rechtsgrundlagen.<sup>4</sup> Damit drängt sich zunächst die Frage auf, warum die gesetzlichen Rechtsgrundlagen diesen zusätzlichen Tatbestand kennen. Die Erklärung hierzu findet sich erneut in dem oben angesprochenen Legitimationsgedanken der gesetzlichen Rechtsgrundlagen.<sup>5</sup>

Die gesetzlichen Rechtsgrundlagen sind Ausdruck einer Interessenabwägung, die auf dem Gedanken fußt, dass der Schutz personenbezogener Daten nicht absolut ist und es somit Interessen an einer Verarbeitung personenbezogener Daten gibt, die diesem Schutzinteresse überwiegen können.<sup>6</sup> Ausgangspunkt dieser Interessenabwägung ist zunächst die Identifikation entsprechender Interessen, die in der Lage sein können, dem Schutzinteresse zu überwiegen. Dies erfolgt bei den gesetzlichen Rechtsgrundlagen durch die Formulierung eines Zweckrahmens, der den Anwendungsbereich der Rechtsgrundlagen einschränkt.<sup>7</sup> Der Zweckrahmen wird dabei entweder durch die Datenschutz-Grundverordnung final festgelegt oder muss durch zusätzliche Methoden weiter konkretisiert werden.<sup>8</sup>

Die Festlegung schutzwürdiger Interessen an einer Datenverarbeitung kann jedoch nicht ausreichen, um die Abwägung zugunsten einer Verarbeitung zu

---

<sup>3</sup> Spindler/Schuster/*Spindler/Dalby*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 6 DS-GVO, Rn. 4; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 13, 19; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 15; Ulmer-Eilfort/Obergfell/*Herbort*, Verlagsrecht, 2. Aufl. 2021, 1. Kapitel, I., Rn. 1075; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 8; DatKomm/*Kastelitz/Hötzendorfer/Tschohl*, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19.

<sup>4</sup> DatKomm/*Kastelitz/Hötzendorfer/Tschohl*, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 15, „übergreifende Prinzip der Erforderlichkeit“; auch Taeger/Gabel/*Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 23; ebenso Ulmer-Eilfort/Obergfell/*Herbort*, Verlagsrecht, 2. Aufl. 2021, 1. Kapitel, I., Rn. 1075 und Paal/Pauly/*Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 9.

<sup>5</sup> Siehe hierzu: Kap. 8, C. *Der Legitimationsgedanke hinter den Rechtsgrundlagen*.

<sup>6</sup> Siehe hierzu: Kap. 8, C., III. *Die gesetzlichen Rechtsgrundlagen als vordefinierte Eingriffsrechtfertigung*.

<sup>7</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen* und Kap. 8, C., III., 2. *Verwirklichung der Abwägung*.

<sup>8</sup> Siehe hierzu: Kap. 8, C., III., 2. *Verwirklichung der Abwägung*.

entscheiden. Um abwägen zu können, ob das Interesse an der Verarbeitung dem Schutzinteresse überwiegt, muss auch die konkrete Datenverarbeitung in die Untersuchung mit aufgenommen werden. An dieser Stelle setzt der Tatbestand der Erforderlichkeit an. Dem Tatbestand kommt damit eine zusätzliche Einschränkung der gesetzlichen Rechtsgrundlagen zu.<sup>9</sup> Wie diese Einschränkung jedoch genau wirkt, bedarf einer näheren Betrachtung dessen Funktionsweise.

## B. Bezugspunkte des Tatbestands

### I. Die Erforderlichkeit als Bindeglied

Bevor man sich mit dem inhaltlichen Aussagegehalt des Tatbestands auseinandersetzen kann, muss man sich zunächst mit dessen systematischer Funktion auseinandersetzen. Denn der Begriff „*erforderlich*“ fungiert als Bindeglied zweier Aspekte, die ins Verhältnis zueinander gesetzt und bewertet werden.<sup>10</sup> Um bestimmen zu können, ob etwas erforderlich ist, muss man zunächst klären, was denn dieses „etwas“ (Bezugspunkt 1) überhaupt ist. Durch den Tatbestand der Erforderlichkeit wird der 1. Bezugspunkt sodann ins Verhältnis zum 2. Bezugspunkt gesetzt, um zu bestimmen, ob der 1. Bezugspunkt in Relation zum 2. Bezugspunkt entsprechend erforderlich ist oder nicht. Es geht somit um einen Vergleich zwischen zwei Bezugspunkten, um die Erforderlichkeit zu bestimmen. Eine Auslegung der Erforderlichkeit muss daher bei diesen beiden Bezugspunkten anfangen, in die der Tatbestand zwingend eingebettet ist.

Welche beiden Bezugspunkte dem Tatbestand der Erforderlichkeit zugrunde liegen, kommt aufgrund des Satzbaus besonders schön aus der englischen Sprachfassung des Art. 6 Abs. 1 UAbs. 1 DS-GVO hervor:

---

<sup>9</sup> Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 429.

<sup>10</sup> BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15, als „*Abhängigkeitsbeziehung*“ eingeordnet, mit Verweis auf Albers, Informationelle Selbstbestimmung, 2005, S. 516 f., noch zur Rechtslage vor der Datenschutz-Grundverordnung und wohl eher insgesamt mit Fokus auf das nationale Grundrecht der informationellen Selbstbestimmung; ähnlich Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 43; v. Lewinski/Rüpkke/Eckhardt, Datenschutzrecht, 2. Aufl. 2022, § 12, Rn. 17, „*Verkopplung*“; Herfurth, ZD 2018, S. 514, 515, „*Zweck-Mittel-Relation*“.

“Processing shall be lawful only if and to the extent that at least one of the following applies:

- a) [...]
- b) processing is necessary for the performance of a contract [...];
- c) processing is necessary for compliance with a legal obligation [...];
- d) processing is necessary in order to protect the vital interests [...];
- e) processing is necessary for the performance of a task carried out in the public interest [...];
- f) processing is necessary for the purposes of the legitimate interests [...].”<sup>11</sup>

## II. Die Datenverarbeitung als erster Bezugspunkt

Der erste Bezugspunkt und damit der Aspekt, dessen Erforderlichkeit es gilt zu bewerten, dürfte recht unproblematisch aus dem Verordnungstext ablesbar sein. So ist es die Verarbeitung der personenbezogenen Daten, die erforderlich sein muss.<sup>12</sup>

Wie bereits oben dargestellt,<sup>13</sup> ist die Einbeziehung der konkreten Datenverarbeitung im Lichte der, den gesetzlichen Rechtsgrundlagen zugrundeliegenden, Interessenabwägung zwingend. Denn nur anhand der Datenverarbeitung lassen sich die Auswirkungen auf die Interessen der betroffenen Person am Schutz ihrer personenbezogenen Daten qualifizieren und für die nachfolgende Abwägung bewerten.

<sup>11</sup> Hervorhebungen durch Verfasser.

<sup>12</sup> Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 9; Ulmer-Eilfort/Obergfell/Herbort, Verlagsrecht, 2. Aufl. 2021, 1. Kapitel, I., Rn 1075; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 13; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 15; DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 38.

<sup>13</sup> Siehe hierzu: Kap. 8, C., III., 1. Die gesetzlichen Rechtsgrundlagen als Ausdruck einer Grundrechtsabwägung.

### *III. Der Zweck als zweiter Bezugspunkt*

Auch der zweite Bezugspunkt lässt sich, jedenfalls in seinen groben Zügen, recht schnell aus den jeweiligen gesetzlichen Rechtsgrundlagen ablesen. Am Beispiel des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO, muss verkürzt gesagt die Datenverarbeitung erforderlich sein, für die Erfüllung eines Vertrages. Der zweite Bezugspunkt steht damit im Zusammenhang mit den Zweckrahmen der jeweiligen, gesetzlichen Rechtsgrundlagen. Auch dies ist wieder im Lichte des Legitimationsgedanken vollkommen nachvollziehbar, denn die Verarbeitungszwecke beinhalten ja das in Frage stehende Interesse an der Verarbeitung. Der Tatbestand der Erforderlichkeit setzt diese beiden Aspekte nun ins Verhältnis zueinander, wonach die Datenverarbeitung erforderlich für die Verarbeitungszwecke sein muss. Hinter dieser Prüfung steht nichts anderes als die Frage, ob der Eingriff in das Interesse der betroffenen Personen erforderlich zur Verwirklichung der Interessen an der Verarbeitung ist.

#### *1. Zweckrahmen der Rechtsgrundlage oder Zweck der Verarbeitung*

Im Detail wirft der zweite Bezugspunkt allerdings die Frage auf, was genau von ihm umfasst ist. Hier könnte wieder die Differenzierung zwischen dem Zweck der Verarbeitung und den Zweckrahmen der einzelnen Rechtsgrundlagen von Bedeutung sein. Muss die Datenverarbeitung damit hinsichtlich des jeweiligen Zweckrahmens oder des konkreten Verarbeitungszwecks erforderlich sein? Der Frage nach dem konkreten zweiten Bezugspunkt kommt gleich zweifach eine wesentliche Bedeutung zu.

Stellt man lediglich auf den abstrakteren Zweckrahmen ab, so dürfte dies auch mittelbar Auswirkungen auf den Inhalt des Tatbestands der Erforderlichkeit haben. Die Erforderlichkeit der Datenverarbeitung erfolgt dann anhand des weiter gefassten Zweckrahmens, weshalb dann wohl auch – unabhängig davon wie man die Erforderlichkeit inhaltlich auslegt – die Erforderlichkeit schneller angenommen werden kann, als würde man auf den konkreten Zweck der Verarbeitung abstellen.

Neben diesen inhaltlichen Auswirkungen erlangt die Frage auch konkret für den vorgenommenen Untersuchungsablauf an Bedeutung. Eine Anknüpfung an den Zweckrahmen hätte zur Folge, dass damit auch der Wahl der Rechtsgrundlage – die oben als zweitrangig dargestellt wurde –<sup>14</sup> eine entscheidende

---

<sup>14</sup> Siehe hierzu: Kap. 9, C. *Die Frage einschlägiger Rechtsgrundlagen.*

Bedeutung zukommt. Denn aufgrund der Anknüpfung an den Zweckrahmen einer jeweiligen Rechtsgrundlage hätte dies auch Einfluss auf die Auslegung der Erforderlichkeit selbst. Dann sollte aber auch die Frage geklärt werden, welche Rechtsgrundlage und damit welcher Zweckrahmen für datenverarbeitende TOM (vorrangig) in Betracht käme. Knüpft man hingegen direkt an den konkreten Verarbeitungszweck an, dann wäre dies weitgehend von der Auswahl der Rechtsgrundlage losgelöst. Zwar müsste der Verarbeitungszweck dann einmal in den Zweckrahmen einer Rechtsgrundlage fallen und zusätzlich müsste die Datenverarbeitung auch erforderlich für den Zweck der Verarbeitung sein. Die Wahl der Rechtsgrundlage dürfte dann aber nicht die dann noch vorzunehmende Prüfung der Erforderlichkeit beeinflussen.

## 2. Ermittlung des zweiten Bezugspunkts im Wege der Auslegung

In der Literatur wird ganz herrschend die Auffassung vertreten, dass die Erforderlichkeit der Datenverarbeitung anhand ihres Zwecks zu beurteilen ist.<sup>15</sup> Dennoch scheint es gerechtfertigt zu sein, sich diese Einschätzung einmal genauer anzuschauen. Denn hierbei darf nicht aus dem Auge gelassen werden, dass es meist an einer klaren Abgrenzung zwischen dem Zweck der Verarbeitung und dem (hier genannten) Zweckrahmen der jeweiligen Rechtsgrundlagen fehlt. Im Lichte dieser Differenzierung könnte demnach auch die Einschätzung, die Erforderlichkeit beziehe sich auf den Verarbeitungszweck, hier nicht unbedingt übertragbar sein. Die Frage nach dem korrekten zweiten Bezugspunkt des Tatbestands der Erforderlichkeit verdient daher einer näheren Betrachtung.

---

<sup>15</sup> Simitis/Hornung/Spiecker gen. Döhmman/*Roßnagel*, Datenschutzrecht, 2019, Art. 5 DS-GVO, Rn. 67; DatKomm/*Kastelitz/Hötzendorfer/Tschobl*, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19; BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15, 17; Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 20, besonders deutlich in Rn. 42; Ehmann/Selmayr/*Heberlein*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 5; Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 38; Ulmer-Eilfort/Obergfell/*Herbort*, Verlagsrecht, 2. Aufl. 2021, 1. Kapitel, I, Rn 1075; Kühling/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 39, am Beispiel von Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO: „dem konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses“.



*a) Sprachliche Anknüpfung*

Legt man zunächst den Wortlaut der gesetzlichen Rechtsgrundlagen zugrunde, gibt es jedenfalls Anhaltspunkte, die auf eine Anknüpfung an den Zweckrahmen hindeuten könnten.<sup>16</sup> Wie anhand der obigen Darstellung der gesetzlichen Rechtsgrundlage deutlich wird,<sup>17</sup> verbinden alle gesetzlichen Rechtsgrundlagen die Erforderlichkeit der Datenverarbeitung mit ihrem Zweckrahmen. Bspw. muss die Verarbeitung für die Erfüllung eines Vertrages (Zweckrahmen) erforderlich sein.

Ob dies allerdings dahingehend zu verstehen ist, dass der zweite Bezugspunkt des Tatbestands doch der Zweckrahmen der jeweiligen Rechtsgrundlage ist, ist zu bezweifeln. Denn auch hier ist wieder darauf hinzuweisen, dass der Zweck der Verarbeitung in den gesetzlichen Rechtsgrundlagen zwar nicht ausdrücklich benannt ist und dass auch die Datenschutz-Grundverordnung sprachlich nicht klar zwischen dem Verarbeitungszweck und den Zweckrahmen der Rechtsgrundlagen differenziert.<sup>18</sup> Dennoch liegt der Gedanke an einen konkreten Zweck der Verarbeitung als eine Art Ausfüllung des vordefinierten Zweckrahmens allen gesetzlichen Rechtsgrundlagen zugrunde.<sup>19</sup>

Dass die gesetzlichen Rechtsgrundlagen nicht unmittelbar auf den konkreten Zweck der Verarbeitung abstellen, begründet sich dabei vor allem aus ihrer Systematik, die gerade darauf ausgerichtet ist, sprachlich einen Rahmen abzubilden, der eine Subsumtion einer Vielzahl von Zwecken erlaubt.<sup>20</sup> In Anbetracht dessen verwundert es daher auch nicht, dass die Erforderlichkeit – jedenfalls sprachlich – nicht unmittelbar an den Zweck der Verarbeitung anknüpft.

Das bedeutet zwar nicht, dass es dem Gesetzgeber nicht möglich gewesen wäre, eine denkbare Anknüpfung an den konkreten Zweck der Verarbeitung im Wortlaut abzubilden. Dies hätte aber wohl dazu geführt, dass die Formulierungen der gesetzlichen Rechtsgrundlagen deutlich länger und auch komplizierter ausgefallen wären. Eine weitere Klarstellung des zweiten Bezugspunktes könnte

---

<sup>16</sup> A.A. BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 17, die die Anknüpfung an den Zweck wenigstens für lit. e) und f) aus dem Normtext ablesen.

<sup>17</sup> Siehe hierzu: Kap. 10, B., I. *Die Erforderlichkeit als Bindeglied*.

<sup>18</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen*.

<sup>19</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen*.

<sup>20</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen*.

der Gesetzgeber daher unterlassen haben, um die Übersichtlichkeit der gesetzlichen Rechtsgrundlagen zu gewährleisten. Eine Anknüpfung des Tatbestands der Erforderlichkeit an den konkreten Verarbeitungszweck scheidet nach dem Wortlaut daher nicht von vornherein aus.

### *b) Die Systematik des Tatbestands*

Weitere Anhaltspunkte für den zweiten Bezugspunkt könnten sich aus der Systematik des Tatbestands ergeben. Der Tatbestand bezieht sich auf die Erforderlichkeit der Datenverarbeitung. Unproblematisch kommt der Erforderlichkeit damit die Funktion zu, Datenverarbeitungen einzuschränken. Auf Basis dieser Überlegung erscheint es daher fraglich, warum man dann die Erforderlichkeit an dem abstrakteren und auch gewollt weiter gefassten Zweckrahmen ausrichten sollte, anstatt an dem konkreten Verarbeitungszweck. Denn damit wäre zwangsläufig die einschränkende Wirkung des Tatbestands geringer.

Weiterhin führt dies auch zu einer Überprüfung, deren Logik man kaum nachvollziehen könnte. Dies lässt sich am besten anhand eines Beispiels aufzeigen.

*Beim Kauf eines Notebooks gegen Barzahlung verlangt der Verkäufer die Durchführung einer Bonitätsüberprüfung. Diese Datenverarbeitung soll auf Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO gestützt werden. Generell könnte die Überprüfung der Bonität eines Käufers durchaus zur Erfüllung eines Vertrages erforderlich sein.<sup>21</sup> Würde man also die Erforderlichkeit der Datenverarbeitung zur*

---

<sup>21</sup> Als möglicher Fall des lit b): Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 32; Plath/Plath/Struck, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 13; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 89; Kühling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 383; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 47, beziehen dieses Beispiel aber speziell auf die Bonitätsprüfung im Rahmen eines Darlehnsvertrags. A.A. Kuner/Bygrave/Docksey/Kotschy, GDPR, 2020, p. 331, sieht für die „creditworthiness“ eher die Rechtsgrundlag nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO einschlägig; differenzierter Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 47, die eine Bonitätsprüfung bei Bankgeschäften, in denen die Bank in Vorleistung geht, diese wohl (auch) unter Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO fassen, aber für eine Übermittlung von Bonitätsdaten an Dritte entweder die Einwilligung oder Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO verlangen, siehe aber ablehnend trotz Vorleistung des Verantwortlichen beim Versandhandel Rn.

*Bonitätsprüfung anhand des allgemeinen Zweckrahmens von Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO ausrichten, wäre es gut vertretbar hier eine Erforderlichkeit für die Erfüllung (irgend-)eines Vertrags anzunehmen. Für die Erfüllung des hier konkret in Frage stehenden Vertrages muss man allerdings erheblich an der Erforderlichkeit (wie auch immer sie im Detail dann zu bewerten ist) zweifeln. Denn warum muss der Verkäufer eine Bonitätsprüfung bei einem Kauf gegen Barzahlung vornehmen. Es besteht hier für den Verkäufer kein Ausfallrisiko der Forderung, da der Vertrag sofort vollständig abgewickelt werden kann.*

Das Beispiel sollte zeigen, dass es aus allgemeinen, logischen Erwägungen aufgrund der Funktion des Tatbestands nur schwer nachvollziehbar ist, bei der Erforderlichkeit zwar auf die konkrete Datenverarbeitung abzustellen, aber diese ins Verhältnis zum abstrakten und generalisierten Zweckrahmen zu setzen und nicht ebenfalls zum konkreten Verarbeitungszweck.<sup>22</sup>

### *c) Teleologische Erwägungen*

Diese allgemeine Überlegung ist eine vereinfachte Ausformung des Telos des Tatbestands der Erforderlichkeit. Die Erforderlichkeit der Datenverarbeitung dient ihrer Begrenzung. Denn die Datenverarbeitung ist gleichzeitig der Eingriff in die geschützten Interessen der betroffenen Person. Auf diese Ebene projiziert,

---

66; gegen die Anwendung des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 14, im Rahmen von Darlehnsverträgen.

<sup>22</sup> Vgl. Wybitul/Pöppers/Rauer, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 15, die im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO für die Erforderlichkeit den „konkreten Vertragszweck“ für maßgeblich erachten; auch Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 29, der eben auf den konkreten Vertrag abstellt; auch Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 13; auch Klein, Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?, in: FS Taeger, 2020, S. 235, 246 f., ebenso Schulze/Janssen/Kadelbach/Holzsnigel/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 22; ähnlich Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 47, stellt auf den „konkreten Inhalt des (beabsichtigten) Vertrages“ ab; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 39, „dem konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses“; ähnlich auch Feiler/Forgó, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 6 DS-GVO, Rn. 9, „konkreten Zweck des Schuldverhältnisses“.

geht es damit auch um eine Beschränkung dieses Eingriffes. Wie bereits im Rahmen des Legitimationsgedanken der gesetzlichen Rechtsgrundlagen dargelegt, geht es auf Interessenebene um eine Abwägung zwischen den Schutzinteressen der betroffenen Person und der Interessen an einer Verarbeitung.

Diese Abwägung scheint auf einfachgesetzlicher Ebene nun im Tatbestand der Erforderlichkeit ausgedrückt zu werden, indem hiernach zu entscheiden ist, ob und in welchem Umfang in die geschützten Interessen der betroffenen Person eingegriffen werden kann. Überträgt man daher diesen dahinterstehenden Gedanken wieder zurück auf die Tatbestandsebene, wird das (konkrete) Interesse an einer Verarbeitung jedoch durch den Zweck und nicht durch den abstrakteren Zweckrahmen dargestellt. Der Zweckrahmen dient (nur) als eine grobe Einordnung, die dem Rechtsanwender dabei helfen soll, geschützte Interessen für eine Verarbeitung zu identifizieren. Das eigentliche Interesse an der Verarbeitung wird jedoch erst durch den Verarbeitungszweck ausgedrückt.

Um daher entscheiden zu können, ob die jeweilige Datenverarbeitung erforderlich ist, kann es nicht auf den generalisierten Zweckrahmen ankommen. Denn nur anhand einer Abwägung des konkreten Zwecks der Verarbeitung (und dessen dahinterstehenden Interesses) mit der konkreten Datenverarbeitung (und deren Eingriff in die Schutzinteressen der betroffenen Person) lässt sich die Erforderlichkeit der Datenverarbeitung beurteilen.

#### *IV. Zwischenergebnis*

Der Tatbestand der Erforderlichkeit fungiert als Bindeglied zwischen der Datenverarbeitung und ihrem Zweck. Das Ziel ist die Begrenzung der Datenverarbeitung auf den, für den Zweck erforderlichen Umfang. Gleichzeitig verkörpert sich in dem Tatbestand die Abwägung zwischen dem Eingriff in den Schutz betroffener Personen vor einer Datenverarbeitung und dem Interesse des Verantwortlichen an der Verarbeitung auf einfachgesetzlicher Ebene.

## C. Autonome, übergreifende Auslegung

### I. Allgemeines

Das System des Tatbestands der Erforderlichkeit, mit seinen zwei Bezugspunkten der Datenverarbeitung und dem Verarbeitungszweck wurde hier herausgearbeitet. Eine inhaltliche Auseinandersetzung mit dem Begriff der Erforderlichkeit und wann eine solche vorliegt, kann allerdings immer noch nicht erfolgen. Denn vorab stellt sich die Frage, welche Methodik zu dessen Bestimmung anzuwenden ist. In diesem Zusammenhang sind gleich zwei Probleme zu behandeln.

Einmal ist zu klären, ob dem Tatbestand der Erforderlichkeit ein europäisches oder nationales Verständnis zugrunde liegt. Im europäischen Recht gilt der Grundsatz der europäisch autonomen Auslegung.<sup>23</sup> Die Bedeutung eines Wortes aus dem europäischen Recht ist daher grundsätzlich nicht mit dem Wortsinn aus den Rechtsordnungen der Mitgliedstaaten auszulegen, sondern es ist ein europäisch autonomes Verständnis zugrunde zu legen.<sup>24</sup> Lediglich in Ausnahmefällen, bspw. wo der europäische Gesetzgeber auf ein nationales Verständnis verweist,<sup>25</sup> darf ein solches zugrunde gelegt werden.<sup>26</sup>

---

<sup>23</sup> EuGH, Rs. C-66/08 (Kozłowski), ECLI:EU:C:2008:437 = NJW 2008, S. 3201, Rn. 42; EuGH, Rs. C-135/15 (Nikiforidis), ECLI:EU:C:2016:774 = NJW 2017, S. 141, Rn. 28; EuGH, Rs. C-580/21 (EEW Energy from Waste), ECLI:EU:C:2023:304 = BeckRS 2023, 7670, Rn. 23; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 4 ff.; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 80 ff.; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 335 ff.

<sup>24</sup> EuGH, Rs. C-66/08 (Kozłowski), ECLI:EU:C:2008:437 = NJW 2008, S. 3201, Rn. 42; EuGH, Rs. C-135/15 (Nikiforidis), ECLI:EU:C:2016:774 = NJW 2017, S. 141, Rn. 28; EuGH, Rs. C-580/21 (EEW Energy from Waste), ECLI:EU:C:2023:304 = BeckRS 2023, 7670, Rn. 23; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 80; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 6; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 336.

<sup>25</sup> EuGH, Rs. C-66/08 (Kozłowski), ECLI:EU:C:2008:437 = NJW 2008, S. 3201, Rn. 42; EuGH, Rs. C-135/15 (Nikiforidis), ECLI:EU:C:2016:774 = NJW 2017, S. 141, Rn. 28; EuGH, Rs. C-580/21 (EEW Energy from Waste), ECLI:EU:C:2023:304 = BeckRS 2023, 7670, Rn. 23; Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 4, 6; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 80; *Martens*, Methodenlehre des Unionsrechts, 2013, S. 336;

<sup>26</sup> Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 6 f., spricht von einer „*Vermutung*“ für die europäisch autonome Auslegung; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 80,

Der Grundsatz der europäisch autonomen Auslegung könnte allerdings durch das zweite Problem in Frage gestellt werden. Wie dargestellt wurde, müssen die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO durch zusätzliche Rechtsvorschriften ergänzt werden. Diese Ergänzung kann auch durch das nationale Recht der Mitgliedstaaten erfolgen (vgl. Art. 6 Abs. 3 S. 1 lit. b) DS-GVO), was sich auch auf den Tatbestand der Erforderlichkeit auswirken könnte. Unter anderem aus diesem Grund ist daher nicht nur zu klären, welche Methodik zur Auslegung des Tatbestands heranzuziehen ist, sondern auch die Frage, ob diese Methode für sämtliche Rechtsgrundlagen gilt.

Ähnlich wie im Rahmen des zweiten Bezugspunkts der Erforderlichkeit könnte dies nicht nur Auswirkungen auf die Auslegung des Tatbestands an sich haben. Sollte der Tatbestand in den einzelnen Rechtsgrundlagen unterschiedlich auszulegen sein, käme die Auswahl einer Rechtsgrundlage – die hier als nachrangig betrachtet wird –<sup>27</sup> eine wesentliche Bedeutung zu. Die Probleme einer einheitlichen, Rechtsgrundlagen-übergreifenden Auslegung und die anzuwendende Auslegungsmethode sind eng miteinander verbunden. Eine klare Trennung ist im Rahmen der Untersuchung daher nur schwer möglich.

## *II. Der Grundsatz europäisch autonomer Auslegung und der Verweis auf u.a. das nationale Recht*

Überwiegend verweisen die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 DS-GVO nicht auf das nationale Recht der Mitgliedstaaten. Auch andere Hinweise, die ein nationales Verständnis rechtfertigen könnten, bestehen nicht. Daher sollte hier der Grundsatz der europäisch autonomen Auslegung gelten. Problematisch sind allerdings die bereits angesprochenen Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO. Denn diese setzten eine ergänzende Rechtsgrundlage entweder im EU-Recht oder eben im Recht der Mitgliedstaaten voraus. Denkbar wäre daher, dass bei ergänzenden nationalen Rechtsgrundlagen auch der Tatbestand der Erforderlichkeit und dessen Verständnis der Regelungskompetenz des nationalen Gesetzgebers unterfällt.

---

ähnlich, aber sprachlich noch direkter („absolute Regelfall“); wohl etwas großzügiger *Martens*, Methodenlehre des Unionsrechts, 2013, S. 336 f., der die Entscheidung über eine europäisch autonome oder mitgliedstaatliche Auslegung wohl stets am Einzelfall prüfen will.

<sup>27</sup> Siehe hierzu ausführlicher: Kap. 9, C. *Die Frage einschlägiger Rechtsgrundlagen*.

Anhaltspunkte, die in diese Richtung deuten könnten, finden sich in den Anforderungen der Datenschutz-Grundverordnung an die ergänzenden Rechtsgrundlagen aus Art. 6 Abs. 3 DS-GVO. Von besonderer Relevanz dürfte hier vor allem der Art. 6 Abs. 3 S. 3 DS-GVO sein. Die Verordnung führt hier einige Aspekte auf, die im Rahmen der ergänzenden Rechtsgrundlage geregelt werden dürfen. Dazu gehören u.a. Bestimmungen zu der Art der Daten, der Anwendung bestimmter Verarbeitungsverfahren oder auch der Dauer der Speicherung. Anders als die Vorgabe, im Rahmen der ergänzenden Rechtsgrundlage die Zwecke der Verarbeitung zu regeln (Art. 6 Abs. 3 S. 2 DS-GVO), deuten die Bestimmungen in Art. 6 Abs. 3 S. 3 DS-GVO eher dahin, die Modalitäten der jeweiligen Datenverarbeitung zu regeln. Dies ließe sich dahingehend interpretieren, dass die Datenschutz-Grundverordnung hier u.a. den nationalen Gesetzgebern der ergänzenden Rechtsgrundlage die Befugnis einräumt, nicht nur das Verarbeitungsinteresse zu konkretisieren, sondern auch Vorgaben zu machen, wann eine Datenverarbeitung für diese Verarbeitungsinteressen auch erforderlich sind.<sup>28</sup> Dies könnte dann auch dazu führen, dass der Begriff der Erforderlichkeit nicht in allen Fällen europäisch autonom auszulegen ist und dass man innerhalb der ergänzenden Rechtsgrundlagen nach Art. 6 Abs. 3 DS-GVO an eine – wohl im Wege der funktionalen Auslegung –<sup>29</sup> abweichende Auslegung überlegen müsste.

Aus dem Verweis auf u.a. das nationale Recht eine (umfassende) europäisch autonome Auslegung des Begriffs der Erforderlichkeit abzulehnen ist allerdings nicht zwingend. Denn es schließt sich nicht gegenseitig aus, den Tatbestand der Erforderlichkeit europäisch autonom auszulegen und dem Gesetzgeber gleichzeitig die Möglichkeit zu verschaffen, eine Konkretisierung dieses Tatbestands vorzunehmen. Dies ist nämlich dann möglich, wenn man die Anforderungen nach Art. 6 Abs. 3 S. 3 DS-GVO nur als klarstellende Konkretisierungen auf-

---

<sup>28</sup> So wohl BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 62, wobei nicht ganz klar wird, ob u.a. der nationale Gesetzgeber unmittelbar den Tatbestand regeln darf oder dies mittelbar über die Konkretisierung der Verarbeitungszwecke erfolgt (vgl. Rn. 60).

<sup>29</sup> Siehe zur funktionalen Auslegung im Europäischen Recht statt vieler EuGH, verb. Rs. C-403/08, C-429/08 (Football Association Premier League u.a.), ECLI:EU:C:2011:631 = ZUM 2011, S. 803, Rn. 187 f.; Jung/Krebs/Stiegler/*Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81. Siehe hierzu ausführlicher: Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen* und dort die Nachweise in Fn. 142.

fasst, die es dem Rechtsanwender erleichtern sollen, den Umfang der Datenverarbeitung im Rahmen der ergänzenden Rechtsgrundlagen einzuhalten. Dann könnte auch hier die Erforderlichkeit europäisch autonom ausgelegt werden. Anders als bei den anderen gesetzlichen Rechtsgrundlagen müsste dabei der Gesetzgeber der ergänzenden Rechtsgrundlage anhand einer europäischen Auslegung ermitteln, wann eine Datenverarbeitung in seinen Fällen erforderlich ist und dies in die ergänzende Rechtsgrundlage mit aufnehmen. Verantwortliche, die eine Datenverarbeitung unter diese Rechtsgrundlagen subsumieren, haben es hierdurch leichter, die Rechtmäßigkeit ihrer Verarbeitung, also vor allem ihre Erforderlichkeit, zu überprüfen. Denn jedenfalls bei den anderen gesetzlichen Rechtsgrundlagen müsste der Verantwortliche den Tatbestand der Erforderlichkeit entsprechend selbst auslegen und prüfen, ob seine Datenverarbeitung diese Anforderungen erfüllt. In beiden Fällen würde sich aber nichts an dem grundsätzlichen und dann europäisch autonom auszulegenden Maßstab, der Erforderlichkeit ändern.

Eine europäisch autonome Auslegung der Erforderlichkeit wäre zudem vor dem Hintergrund der Ziele der Datenschutz-Grundverordnung, den Datenschutz in der EU weiter zu harmonisieren (vgl. auch ErwG 9 DS-GVO),<sup>30</sup> angebracht. Die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO sind zwar eine wichtige Brücke, den Datenschutz mit der Gesamtrechtsordnung – und damit auch mit dem Recht der Mitgliedstaaten – zu verbinden.<sup>31</sup> Damit ist jedoch eine gewisse Einschränkung dieses Harmonisierungsziels für das europäische Datenschutzrecht verbunden.<sup>32</sup> Aber dann sollte es doch gerade wichtig sein, dass bei der Frage, ob eine Datenverarbeitung erforderlich ist, also wie stark der Schutz personenbezogener Daten im Verhältnis zum Interesse an einer Verarbeitung eingeschränkt werden darf, ein einheitlicher, europäischer Maßstab verwendet wird.

---

<sup>30</sup> Allgemein zum stärkeren Harmonisierungsgedanken der Datenschutz-Grundverordnung: Ehmann/Selmayr/Selmayr/Ehmann, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung DS-GVO, Rn. 79; Schulze/Janssen/Kadelbach/Holzsnagel/Felber, Europarecht, 4. Aufl. 2020, § 38, Rn. 6.

<sup>31</sup> Siehe hierzu: Kap. 8, C., III., 2., b) *Ergänzungsbedürftige Rechtsgrundlagen*.

<sup>32</sup> Siehe zur Gefahr für die Harmonisierung des EU-weiten Datenschutzrechts aufgrund des Art. 6 Abs. 3 DS-GVO: Simitis/Hornung/Spiecker gen. Döhmann/Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 2, wobei er hier auch die Vorteile der Rechtssicherheit und Modernisierungschancen sieht. Siehe auch Forgó/Helfrich/Schneider/Hanloser, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V, Kapitel 1, Rn. 18 f., als „praktische[...] Notwendigkeit“.



Anhaltspunkte dafür finden sich zudem in Art. 6 Abs. 3 DS-GVO selbst wieder. Denn die Verordnung unterscheidet hier wohl zwischen zwingenden und fakultativen Anforderungen.<sup>33</sup> Ausgehend vom Wortlaut („*kann spezifische Bestimmungen [...] enthalten*“)<sup>34</sup> dürften die Anforderungen nach Art. 6 Abs. 3 S. 3 DS-GVO fakultativ sein.<sup>35</sup> Dagegen müssen bspw. die Vorgaben an die Zwecke der Verarbeitung (Art. 6 Abs. 3 S. 2 DS-GVO) zwingend in der ergänzenden Rechtsgrundlage enthalten sein.<sup>36</sup>

---

<sup>33</sup> Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 3; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 37; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 57; Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 216; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 147 ff.

<sup>34</sup> Englisch: „*may contain specific provisions*“, Französisch: „*peut contenir des dispositions spécifiques*“, Spanisch: „*podrá contener disposiciones específicas*“, Italienisch: „*potrebbe contenere disposizioni specifiche*“, Niederländisch: „*kan specifieke bepalingen bevatten*“.

<sup>35</sup> Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 216; Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 57, ausgenommen der zuvor genannten Anforderungen sollen die weiteren Kriterien „*Kann*-Vorgaben“ sein; BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 81, allerdings mit einer anderen Zitierweise (Abs. 3 UAbs. 2 S. 2); Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 12; Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 60; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 150, 172, 176 ff.; Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 39.

<sup>36</sup> Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 57; Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 216; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 120; Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 3 DS-GVO, Rn. 27 f.; Auernhammer/Kramer, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 93; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 149; Ehmann/Selmayr/Heberlein, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rn. 39; Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 37, jedoch mit einer anderen Zitierweise; auch unter Verwendung einer anderen Zitierweise Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 160.

Ohne die Angaben der Verarbeitungszwecke wäre die ergänzende Rechtsgrundlage sinnentleert und könnte überhaupt nicht als eine notwendige Konkretisierung der ergänzungsbedürftigen Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO angesehen werden.<sup>37</sup> Eine Klarstellung des Gesetzgebers der ergänzenden Rechtsgrundlage, wann in diesen Fällen (nach einem europäischen Maßstab) auch von der Erforderlichkeit auszugehen ist, bedarf es hingegen nicht zwingend. Fehlt es hieran in der ergänzenden Rechtsgrundlage, dann müssen Verantwortliche ausgehend von dem Zweck der Verarbeitung die Erforderlichkeit ihrerseits anhand des europäischen Maßstabs bestimmen.

Vorzugswürdiger ist daher, den Tatbestand der Erforderlichkeit europäisch autonom auszulegen.<sup>38</sup> Ein mitgliedstaatliches Verständnis über diesen zentralen Punkt bei den gesetzlichen Rechtsgrundlagen ist abzulehnen. Dem Gesetzgeber einer ergänzenden Rechtsgrundlage kommt daher allenfalls die Kompetenz zu, die Erforderlichkeit anhand des europäisch autonomen Maßstabs zu ermitteln und dann in der ergänzenden Rechtsgrundlage klarzustellen, um die Subsumtion durch den Rechtsanwender zu erleichtern. Hiermit würde man auch die Gefahr für die Harmonisierung eingrenzen, die durch diese Öffnung

---

<sup>37</sup> In eine ähnliche Richtung siehe auch Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 82, indem sie im Kontext des Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO die Zweckfestlegung als „grundlegende Voraussetzung für die Erzeugung einer rechtlichen Verpflichtung“ ansehen.

<sup>38</sup> Im Ergebnis auch: EuGH, Rs. C-524/06 (Huber), ECLI:EU:C:2008:724 = MMR 2009, S. 171, Rn. 52, bereits zum – mit Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO vergleichbaren – Art. 7 lit. e) DS-RL. Auf dieses Urteil beziehend: DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19; Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 118, konkret zur Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO und Verweis auf lit. c) (Rn. 81 f.); ähnlich BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 60 zu Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; Franzen/Gallner/Oetker/Franzen, Eu-ArbRK, 5. Aufl. 2024, 270. Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 2, wohl für die Übertragung auf alle entsprechenden Rechtsgrundlagen des Art. 6 DS-GVO. Siehe ohne ausdrücklichen Verweis auf das zuvor genannte Urteil im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO auch Schwartmann u.a./Jacquemain u.a., DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 100. Siehe auch EDSA, Leitlinien 2/2019, Rn. 23 und dort die Fn. 16, der das Urteil auf Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO überträgt; hierauf Bezug nehmend Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 38.

zugunsten mitgliedstaatlicher Regelungen droht.<sup>39</sup> Denn die Mitgliedstaaten könnten dann zwar weiterhin die rechtliche Verpflichtung bzw. das öffentliche Interesse / die öffentliche Gewalt konkretisieren, müssten sich aber beim Umfang der damit in Verbindung stehenden Datenverarbeitung an dem gemeinsamen, nach europäischem Maßstab zu bemessenen, Tatbestand der Erforderlichkeit halten.

### III. Differenzierung zwischen Auslegungsmaßstab und Auslegungsergebnis

Der Tatbestand der Erforderlichkeit ist europäisch autonom auszulegen. Auch wenn damit ein nationales Verständnis – das für einige der Rechtsgrundlagen denkbar war – abzulehnen ist, beantwortet dies aber noch nicht die Frage, ob es nur eine europäisch autonome Auslegung des Tatbestands der Erforderlichkeit gibt oder aber ob der Begriff innerhalb der einzelnen Rechtsgrundlagen zwar europäisch, aber unterschiedlich auszulegen ist.

Die wissenschaftliche Diskussion widmet sich dem Tatbestand der Erforderlichkeit meist im direkten Zusammenhang mit den einzelnen Rechtsgrundlagen. Dabei wird der Tatbestand oft anhand von denkbaren Beispielen diskutiert und bewertet, ob diese Datenverarbeitungen innerhalb der jeweiligen Rechtsgrundlagen erforderlich sind. Offen bleibt teilweise eine detaillierte Auseinandersetzung des Maßstabs anhand dessen die Erforderlichkeit überhaupt zu ermitteln ist. Aus den getroffene Auslegungsergebnissen einzelner Beispiele lässt sich daher meist nur schwer etwas über das Grundverständnis des Tatbestands der Erforderlichkeit ableiten.

Dazu kommt, dass der Tatbestand wohl häufig im Lichte der jeweiligen Rechtsgrundlagen ausgelegt wird und sich daher zwischen den einzelnen Rechtsgrundlagen unterscheidet.<sup>40</sup> Auch eine Differenzierung anhand des Personenkreises wird diskutiert. So soll der Tatbestand für öffentliche Stellen enger

---

<sup>39</sup> Vgl. auch allgemein Simitis/Hornung/Spiecker gen. Döhmman/*Albrecht*, Datenschutzrecht, 2019, Einführung zu Art. 6 DS-GVO, Rn. 6, der daher keinen großen Raum u.a. für die Mitgliedstaaten sieht, da sie insb. an die Anforderungen des Abs. 3 gebunden sind; siehe auch Paal/*Pauly/Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 43, der ebenfalls darauf verweist, dass den Gesetzgebern ergänzender Rechtsgrundlagen Einschränkungen durch die Datenschutz-Grundverordnung vorgegeben werden.

<sup>40</sup> Siehe Paal/*Pauly/Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 23, mit der Differenzierung zwischen Art. 6 Abs. 1 UAbs. 1 lit. b) und e) DS-GVO; ähnlich *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 402; siehe auch die Differenzierung

auszulegen sein als für nicht öffentliche Stellen.<sup>41</sup> Wobei die Differenzierung nach Personenkreisen in einigen Fällen wohl faktisch auf die Ebene der Rechtsgrundlagen durchschlagen dürfte. So gilt bspw. nach Art. 6 Abs. 1 UAbs. 2 DS-GVO die Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO) nicht für Behörden in Erfüllung ihrer Aufgaben.<sup>42</sup> Dagegen soll Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO (vorrangig)<sup>43</sup> öffentlichen Stellen zur Verfügung stehen.<sup>44</sup>

Im Folgenden soll daher anhand der – hier relevanten – europäischen Methodik der Frage nachgegangen werden, ob der Tatbestand der Erforderlichkeit

---

zwischen lit. b) und f) auf der einen und lit. c) und e) auf der anderen Seite Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 58, 75, 100, 107, 151; Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 94, der scheinbar für die Erforderlichkeit i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO strengere Anforderungen stellt (vgl. auch dagegen Rn. 57). Siehe auch DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19, die für eine Differenzierung sowohl nach Rechtsgrundlagen als auch Personengruppen (hierzu sogleich) abstellen, wodurch sich aber die enge Verbindung zwischen beiden zeigt (hierzu ebenfalls sogleich); Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 33, möchte die Erforderlichkeit im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO strenger als unter lit. b) auslegen.

<sup>41</sup> Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 9, spricht von „*unterschiedliche Wirkungen*“; vgl. DatKomm/Kastelitz/Hötzendorfer/Tschobl, Stand: 76. EL. 2023, Art. 6 DS-GVO (Stand: Juli 2020), Rn. 19; siehe wohl auch *v. Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 12, Rn. 33 ff., insb. Rn. 36 f., die bei den Auswirkungen der Erforderlichkeit verschiedene Konstellationen benennen, von der eine die „*öffentliche Verwaltung*“ ist.

<sup>42</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 65; Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 157 f.; Gierschmann u.a./*Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 123; *Ziegenhorn/v. Heckel*, NVwZ 2016, S. 1585, 1587; *Veil*, NJW 2018, S. 3337, 3338.

<sup>43</sup> Personen des Privatrechts sind zwar nicht vollständig ausgeschlossen, müssen aber eben eine Aufgabe im *öffentlichen* Interesse erfüllen, deren Erfüllung ihr vorab übertragen wurde, vgl. Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 23.

<sup>44</sup> Vgl. hinsichtlich des Fokus auf öffentliche Stellen: Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 51; Gierschmann u.a./*Assion/Nolte/Veil*, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 27, die die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO eher dem öffentlichen und die anderen Rechtsgrundlagen eher dem privaten Bereich zuordnen.

generell und insbesondere in Abhängigkeit der jeweiligen Rechtsgrundlage unterschiedlich auszulegen ist.

Neben dem Grundsatz der europäisch autonomen Auslegung ist grundsätzlich anzunehmen, dass derselbe Begriff innerhalb eines Rechtsakts identisch auszulegen ist.<sup>45</sup> In der Ausgangslage spräche dies erstmal gegen eine unterschiedliche Auslegung des Begriffs der Erforderlichkeit innerhalb der einzelnen Rechtsgrundlagen. Eine – im Wege der funktionalen Auslegung – abweichende Auslegung wäre möglich, wenn demselben Begriff (auch innerhalb desselben Rechtsakts) unterschiedliche Funktionen zukommen.<sup>46</sup> In diesen Fällen ist anhand des Telos eine abweichende Auslegung zu ermitteln, die der jeweiligen Funktion des Tatbestands Rechnung trägt. Als Ausnahme vom Grundfall bedarf es für eine solche Abweichung allerdings einer besonderen Rechtfertigung. Ob eine solche Rechtfertigung hier gegeben ist, mag jedoch zu bezweifeln sein.

So ist doch zu beachten, dass das Unionsrecht den Begriff der Erforderlichkeit nicht nur im Rahmen desselben Rechtsakts verwendet, sondern innerhalb dieses Rechtsakts auch im selben System, welches die Rechtmäßigkeit einer Datenverarbeitung regelt. Es ist nur schwer anzunehmen, dass der europäische Gesetzgeber in diesem Zusammenhang zwar denselben Begriff verwendet, diesem aber in den jeweiligen Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO eine andere Bedeutung zumessen möchte. Weiterhin ist, wie oben bereits herausgearbeitet

---

<sup>45</sup> Vgl. *Jung*, Spezifika der europäischen Methodenlehre, in: Das Vorabentscheidungsverfahren in der Zivilgerichtsbarkeit, 2014, S. 17, 21 und *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81, die ein einheitliches Verständnis innerhalb des gesamten Rechtsakts wenigstens für definierte Begriffe grds. annehmen; siehe auch EuGH, Rs. C-128/11 (*UsedSoft*), ECLI:EU:C:2012:407 = ZUM 2012, S. 661, Rn. 60 und EuGH, verb. Rs. C-403/08, C-429/08 (*Football Association Premier League u.a.*), ECLI:EU:C:2011:631 = ZUM 2011, S. 803, Rn. 187 f., wonach der EuGH von dem Grundfall ausgeht, dass die Begriffe zweier, miteinander verwandter Richtlinien dieselbe Bedeutung haben sollten; hierzu auch *Riesenhuber/Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 20, der zwar grds. auf die „*Relativität der Rechtsbegriffe*“ abstellt, aber bei fortgeschritten harmonisierten Rechtsbereichen eine, zwischen den Rechtsakten abweichende Bedeutung nicht vermutet. Für die einheitliche Bedeutung desselben Begriffs innerhalb eines Rechtsakts dürfte dies daher umso eher gelten.

<sup>46</sup> Siehe zur funktionalen Auslegung im Europäischen Recht statt vieler EuGH, verb. Rs. C-403/08, C-429/08 (*Football Association Premier League u.a.*), ECLI:EU:C:2011:631 = ZUM 2011, S. 803, Rn. 187 f.; *Jung/Krebs/Stiegler/Krebs/Jung*, Gesellschaftsrecht in Europa, 2019, § 2 Europäische Rechtsmethodik, Rn. 81. Siehe hierzu ausführlicher: Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen* und dort die Nachweise in Fn. 142.

wurde, die Funktion des Tatbestands in allen gesetzlichen Rechtsgrundlagen dieselbe.<sup>47</sup> Zudem greift der Tatbestand der Erforderlichkeit in seiner Funktion dabei noch nicht mal auf die jeweilige Rechtsgrundlage zurück, indem er bspw. an deren Zweckrahmen anknüpft. Die Bezugspunkte des Tatbestands sind die Datenverarbeitung und der konkrete Zweck der Verarbeitung. Der Zweck spielt zwar auch eine Rolle bei der „Wahl“ der jeweiligen Rechtsgrundlage. Die Erforderlichkeit kann allerdings losgelöst davon beurteilt werden.

Ohne die Funktion der Rechtsgrundlagen zu beeinträchtigen, wäre es möglich gewesen, Art. 6 Abs. 1 UAbs. 1 DS-GVO so aufzubauen, dass der Tatbestand der Erforderlichkeit für alle gesetzlichen Rechtsgrundlagen „vor die Klammer gezogen wird“. Wenn der Tatbestand der Erforderlichkeit allerdings weitgehend losgelöst von der jeweiligen Rechtsgrundlage geprüft werden kann, muss auch eine daran ausgerichtete Differenzierung bei der Auslegung des Tatbestands ausscheiden. Es gibt daher keine Anhaltspunkte, die eine funktionale Auslegung rechtfertigen, den Tatbestand der Erforderlichkeit für jede Rechtsgrundlage einzeln auszulegen.

#### *IV. Zwischenergebnis*

Der Maßstab für die Ermittlung der Erforderlichkeit ist damit Rechtsgrundlagen-übergreifend einheitlich, europäisch autonom auszulegen. Das Ergebnis dieser Auslegung wird sich zwar unterscheiden können, dies liegt aber in der Funktion des Tatbestands begründet, der zwei variable Bezugspunkte ins Verhältnis setzt und nicht daran, dass der Maßstab für die Bewertung der Erforderlichkeit innerhalb der einzelnen Rechtsgrundlagen abweicht. Es handelt sich insofern um einen dynamischen und nicht um einen fixen Tatbestand.

### D. Auslegung der Erforderlichkeit

Nachfolgend sollen verschiedenen Ansätze in der Diskussion um die Auslegung des Tatbestands der Erforderlichkeit dargestellt werden. Ein Problem bei der Darstellung dieses Diskussionsstands liegt dabei einmal in der teilweise vorgenommenen Erörterung anhand von Einzelfällen. Ferner kommt hinzu, dass für

---

<sup>47</sup> Siehe hierzu: Kap. 10, B. *Bezugspunkte des Tatbestands*.

die jeweiligen Rechtsgrundlagen wohl unterschiedliche Auslegungen des Tatbestands befürwortet werden, was hier jedoch abgelehnt wird.<sup>48</sup> Die nachfolgende Darstellung denkbarer Bewertungsmaßstäbe für die Auslegung des Tatbestands der Erforderlichkeit erfolgen daher nur allgemein. Mögliche Ansätze werden daher, in Übereinstimmung mit den zuvor erarbeiteten Ergebnissen, für alle gesetzlichen Rechtsgrundlagen zusammengefasst.

### *I. Denkbare Bewertungsmaßstäbe*

Aus der Diskussion über die Auslegung des Tatbestands der Erforderlichkeit lassen sich unterschiedliche Anknüpfungspunkte für die Bestimmung dieser erkennen. Diese unterschiedlichen Ansätze schließen sich nicht zwingend aus und werden (teilweise) sogar in der Diskussion miteinander kombiniert. Für ein besseres Verständnis der einzelnen Ansätze und ihrer möglichen Verbindung werden sie nachfolgend jedoch erstmal getrennt voneinander dargestellt.

#### *1. Alternativen zur Datenverarbeitung*

Ob eine Datenverarbeitung als erforderlich anzusehen ist, soll vielfach daran zu beurteilen sein, ob sich der Zweck der Verarbeitung auch auf andere Weise erreichen lässt. Dieser Bewertungsmaßstab legt daher den Fokus auf Alternativen zur geplanten Datenverarbeitung. Wann eine Datenverarbeitung nach diesem Bewertungsmaßstab als erforderlich anzusehen ist, wenn Alternativen zur ihr vorliegen, wird in der Diskussion weiter differenziert.

Nach der strengeren Ansicht innerhalb dieses Bewertungsmaßstabs ist die Grenze für die Erforderlichkeit bereits dort zu ziehen, wo der Zweck ohne die Verarbeitung nicht erreicht werden kann.<sup>49</sup> Kann der Zweck also auf anderem Wege erreicht werden, fehlt es an der Erforderlichkeit.

---

<sup>48</sup> Siehe hierzu: Kap. 10, C., III. *Differenzierung zwischen Auslegungsmaßstab und Auslegungsergebnis*.

<sup>49</sup> Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 9, für Privatrechtssubjekte sollen aber wohl weniger strenge Anforderungen gelten (vgl. Rn. 14); Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 100 zu Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO, wonach es nicht darauf ankäme, ob das „*mildere Mittel wirtschaftlich sinnvoll*“ wäre; so wohl auch Kuner/Bygrave/Docksey/Kotschy, GDPR, 2020, p. 331, anhand von lit. b), stellt aber wohl auf das Fehlen realistischer (und nicht nur theoretischer) Alternativen ab.

Während die erste Ansicht hier wohl die Erforderlichkeit bei irgendeiner Alternative zur Datenverarbeitung ablehnt, dürfte eine großzügigere Ansicht die Grenze der Erforderlichkeit beim Vorliegen von Alternativen erst dort ziehen, wo es keine zumutbaren Alternativen gibt, den Zweck der Verarbeitung zu erreichen (vgl. auch ErwG 39 S. 9 DS-GVO).<sup>50</sup> Anders als nach dem ersten Bewertungsmaßstab können hier auch trotz Alternativen Datenverarbeitungen erforderlich sein. Denn eine Erforderlichkeit der Datenverarbeitung scheidet nicht mehr nur aus, wenn bereits irgendeine Alternative zur Datenverarbeitung besteht, sondern mögliche Alternativen müssen für den Verantwortlichen auch zumutbar sein. Der Maßstab nimmt damit eine qualitative Bewertung möglicher Alternativen in die Betrachtung mit ein.

## 2. Qualifizierung der Zweckerreichung

Ein zweiter Bewertungsmaßstab für die Erforderlichkeit erfolgt nicht unmittelbar aus dem Blickwinkel der Datenverarbeitung und hierzu bestehender Alternativen, sondern rückt den Zweck der Verarbeitung in den Fokus der Betrachtung. Die Erforderlichkeit der Datenverarbeitung bemisst sich hieran, welchen Beitrag sie leistet, um den Zweck der Verarbeitung zu erreichen.

---

<sup>50</sup> Gola/Heckmann/*Schulz*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 20; Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 434; Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 8 f.; Plath/*Plath/Struck*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 17 ff., insb. Rn. 21; Sydow/Marsch/*Reimer*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 27, anhand des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO; Specht/Mantz/*Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 54; Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 42, zu Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO; Wybitul/*Pöiters/Rauer*, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 46, zu Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; Kühling/*Buchner/Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 15, an anderer Stelle befürworten sie eine enge Auslegung des Tatbestands (Rn. 38), stellen aber nicht auf die „*absolut zwingende Notwendigkeit*“ ab (Rn. 45); abstellend auf die Zumutbarkeit bei Privatrechtssubjekten Paal/*Pauly/Frenzel*, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO, Rn. 14, im Zusammenhang der Erforderlichkeit bei vertraglichen Interessen, siehe allerdings auch in eine strengere Richtung (Rn. 9).



Nach wohl herrschender Ansicht dürfte es nicht ausreichend sein, wenn die Datenverarbeitung für die Erreichung des Zwecks (nur) förderlich ist.<sup>51</sup> Fraglich bleibt damit, ob eine Datenverarbeitung nur dann erforderlich ist, wenn sie den Zweck (irgendwie) erreicht oder ob sie auch hierüber hinaus gehen darf. So wird auch darauf verwiesen, dass eine Datenverarbeitung auch (noch) erforderlich ist, wenn sie den Zweck der Verarbeitung effektiv erreicht.<sup>52</sup> Weiterhin hat der EuGH die Erforderlichkeit der Datenverarbeitung aber auch angenommen, wenn sie den Zweck<sup>53</sup> effizienter erreicht.<sup>54</sup>

---

<sup>51</sup> Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, allgemein in Rn. 15, zu Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO in Rn. 42 und zu Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO in Rn. 147c; Specht/Mantz/*Mantz/Marosi*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019, § 3, Rn. 54; Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 43, zu Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO; auch zu Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO *Klaas*, CCZ 2020, S. 256, 259; ebenfalls *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 384. Differenzierter *Plath/Plath/Struck*, DSGVO/BDSG/TDSDG, 4. Aufl. 2023, Art. 6 DS-GVO, Rn. 22. A.A. Schuster/Grützmacher/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 30, bezüglich Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO; wohl auch allgemein Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 432 f., der es wohl ausreichen lässt, die „Zweckerreichung zu erleichtern“, in eine andere Richtung dann allerdings in Rn. 646 im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO, wonach eine „Dienlichkeit“ wohl nicht ausreichen dürfte.

<sup>52</sup> Vgl. Simitis/Hornung/Spiecker gen. Döhmman/*Rofsnagel*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 77, spricht jedoch konkret von der effektiven Wahrnehmung der Aufgabe i.S.d. Art. 6 Abs. 1 lit. e) DS-GVO; *Herfurth*, ZD 2018, S. 514, 515, spricht ebenfalls im Rahmen einer Kombination (hierzu sogleich) von der effektiven Wahrnehmung von Interessen im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO „zur Interessenswahrung geeignet ist und keine mildere, gleich effektive Alternative besteht“; ähnlich im Zusammenhang einer Kombination und mit Verweis auf „Interessen“ Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 147c und auch zu Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO. Siehe auch hinsichtlich einer vergleichbaren Art der Qualifizierung der Zweckerreichung Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 432, „keine [später: „datenschutzschonender[e]“] alternative Form der Datenverarbeitung besteht, die die Zwecke in vergleichbarer Weise erreichen kann“ und Rn. 434; siehe ferner Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 43, stellt wohl, ebenfalls in Kombination, im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO auf das „hinreichend[e]“ Erreichen des Vertragszwecks ab, worin ebenfalls eine Art Qualifizierung gesehen werden kann.

<sup>53</sup> In den Fällen ging es konkret um die effizientere Anwendung von Rechtsvorschriften im Zusammenhang des Art. 7 Abs. 1 lit. e) DS-RL.

<sup>54</sup> Vgl. EuGH, Rs. C-524/06 (Huber), ECLI:EU:C:2008:724 = MMR 2009, S. 171, Rn. 62; EuGH, Rs. C-342/12 (Worten), ECLI:EU:C:2013:355 = ZD 2013, S. 437, Rn. 37, beide noch

Die Bewertungen anhand von Alternativen zur Datenverarbeitung und der Qualität, den Verarbeitungszweck zu erreichen, schließen sich nicht gegenseitig aus. So könnte man die Erforderlichkeit einer Datenverarbeitung auch annehmen, wenn es keine zumutbaren Alternativen gibt, den Zweck gleich effektiv zu erreichen.<sup>55</sup> Gerade in Bezug auf die Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. c) und e) DS-GVO wird aufgrund der Bindung an eine gesetzliche, ergänzende Rechtsgrundlage im Rahmen der Erforderlichkeit auf den (verfassungsrechtlichen) Grundsatz der Verhältnismäßigkeit abgestellt, wonach es kein milderes Mittel geben darf, den Zweck gleich effektiv zu erreichen.<sup>56</sup> Zwar geht

---

zur DS-RL. Mit Verweis auf die Rechtsprechung des EuGH: Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 119, im Zusammenhang der Erforderlichkeit nach Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; auch Simitis/Hornung/Spiecker gen. Döhmann/*Rofsnagel*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 77; ebenso Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 100, 107. A.A. wohl Simitis/Hornung/Spiecker gen. Döhmann/*Schantz*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 36, der im Kontext des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO die effizientere Vertragserfüllung für nicht erforderlich hält.

<sup>55</sup> Vgl., jedoch eben nicht mit Bezug auf den Zweck, sondern dem Begriff „Interesse“: *Herfurth*, ZD 2018, S. 514, 515, „keine mildere, gleich effektive Alternative“ zu Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; ähnlich Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 147c. Siehe auch die kombinierte Berücksichtigung beider Ansätze Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 432, „keine [später: „datenschutzschonender[e]“] alternative Form der Datenverarbeitung besteht, die die Zwecke in vergleichbarer Weise erreichen kann“ und Rn. 434; ebenfalls mit einer Kombination beider Ansätze Auernhammer/*Kramer*, 8. Aufl. 2024, Art. 6 DS-GVO, Rn. 43, „keine [...] mildere Verarbeitung [...] um den Zweck des Vertrages [...] hinreichend zu erreichen“.

<sup>56</sup> Mit Verweis auf die Verhältnismäßigkeit: Schwartmann u.a./*Jacquemain u.a.*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 75, 100, 107; Taeger/*Gabel/Taeger*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 94, zu Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 402, zu Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; *Kuner/Bygrave/Docksey/Kotschy*, GDPR, 2020, p. 336, mit dem Verweis auf „proportionality“ im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; siehe auch *Robrahn/Bremert*, ZD 2018, S. 291, 292, für die Anwendung auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; siehe *Wybitul/Pötters/Rauer*, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 16, für eine Verhältnismäßigkeitsprüfung im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO. Siehe allgemein zum Verhältnis der Erforderlichkeit mit dem Grundsatz der Verhältnismäßigkeit Schantz/Wolff/*Wolff*, Das neue Datenschutzrecht, 2017, Rn. 430, der von „weitgehende[n] Übereinstimmungen“ spricht. Siehe auch *Franzen/Gallner/Oetker/Franzen*, EuArbRK, 5. Aufl. 2024, 270. Datenschutz-Grundverordnung, Art. 6 DS-GVO, Rn. 2, der für alle Rechtsgrundlagen des Art. 6 Abs. 1 UAbs. 1 DS-GVO die „Anwendung des

es dort nicht um ein zumutbares Mittel (bzw. eine zumutbare Alternative), allerdings zeigt sich hieran, dass beide Bewertungsmaßstäbe miteinander kombiniert werden können.

### 3. Verhältnis zwischen Datenverarbeitung und Zweck

Der hier dritte Bewertungsmaßstab rückt das Verhältnis zwischen der Datenverarbeitung und dem Zweck in den Vordergrund. Die Erforderlichkeit ist demnach daran zu messen, ob der Zweck ohne die Datenverarbeitung (bzw. konkreter ohne den jeweiligen Verarbeitungsschritt)<sup>57</sup> erreicht werden kann.<sup>58</sup> Auf mögliche Alternativen soll es dabei (vorrangig) nicht ankommen.<sup>59</sup> Damit einher geht aber eine – wie die Vertreter dieser Ansicht beschreiben – „gewisse Bandbreite“.<sup>60</sup> In diesem Rahmen sollen sich dann auch „Betroffenheits- und Interessenkonstellationen“ berücksichtigen lassen.<sup>61</sup> Im Endeffekt dürfte dies daher darauf hinauslaufen, dass nach dieser Ansicht dem Tatbestand der Erforderlichkeit auch eine Art Interessenabwägung zugrunde liegt, bei der ein Ausgleich gefunden werden muss zwischen dem Interesse am Zweck der Verarbeitung und dem Interesse am Schutz vor einer Verarbeitung.

---

Verhältnismäßigkeitsgrundsatzes“ als „immanent“ ansieht und direkt im Anschluss die Erforderlichkeit anspricht.

<sup>57</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 18, „*Verarbeitungsschritt*“ oder auch „*Verarbeitungsvorgang*“ (Rn. 19); siehe bereits zur Rechtslage vor der Datenschutz-Grundverordnung und wohl mit Fokus auf das nationale Grundrecht der informationellen Selbstbestimmung *Albers*, Informationelle Selbstbestimmung, 2005, S. 517, die dort bereits vom „*jeweiligen Verarbeitungsvorgang*“ und „*jeweilige[n] Verarbeitungsschritt*“ (S. 518) spricht.

<sup>58</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15; siehe bereits *Albers*, Informationelle Selbstbestimmung, 2005, S. 517.

<sup>59</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 15, 19; siehe bereits zur Rechtslage vor der Datenschutz-Grundverordnung und wohl mit Fokus auf das nationale Grundrecht der informationellen Selbstbestimmung *Albers*, Informationelle Selbstbestimmung, 2005, S. 517. Siehe aber zu der hier vertretenen Orientierungshilfe insbesondere von Alternativen noch sogleich: Kap. 10, D., III. *Würdigung der Bewertungsmaßstäbe und eigene Lösung*.

<sup>60</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 19.

<sup>61</sup> BeckOK Datenschutzrecht/*Albers/Veit*, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 19.

## II. Eigene Auslegung

Abhängig von dem zugrunde gelegten Bewertungsmaßstab kann es zu deutlich abweichenden Ergebnissen führen, wann eine Datenverarbeitung als erforderlich und damit auch als rechtmäßig anzusehen ist. Dem Tatbestand kommt damit eine überragende Bedeutung im allgemeinen System der Rechtsgrundlagen zu. Für die hier untersuchten Datenverarbeitungen entscheidet dabei der Tatbestand im Wesentlichen darüber, ob datenverarbeitende TOM rechtlich implementiert werden dürfen.

Eine Antwort auf die Frage, welcher Bewertungsmaßstab dem Tatbestand zugrunde zu legen ist, ist damit zwingend für die weitere Untersuchung und vor allem für die Erarbeitung eines Lösungsvorschlags für das Spannungsverhältnis zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle. Bevor die hier dargestellten Bewertungsmaßstäbe kritisch gewürdigt werden, soll anhand einer eigenen Auslegung ermittelt werden, welchen Maßstab die Datenschutz-Grundverordnung für die Erforderlichkeit ansetzt. Anschließend soll das eigene Auslegungsergebnis mit den dargestellten Bewertungsmaßstäben verglichen und gemeinsam mit ihnen bewertet werden.

### 1. Wortlaut

Den Anfang für die Auslegung bildet wie immer der Wortlaut.<sup>62</sup> Ausgehend von einem europäisch autonomen Verständnis kommt es bei der Wortlautauslegung zunächst darauf an, wie die Begriffe für „erforderlich“ in den verschiedenen Sprachfassungen verwendet werden. Der Begriff „erforderlich“ (engl. „necessary“)<sup>63</sup> beschreibt in seiner gewöhnlichen Verwendung wohl überwiegend, dass etwas *unerlässlich* vorliegen *muss*. Im allgemeinen Sprachgebrauch drängt sich dabei ein zwingender Charakter für das Vorliegen einer Bedingung auf. Auch die anderen, untersuchten Sprachfassungen legen ein solches Verständnis nahe.<sup>64</sup>

---

<sup>62</sup> Zum Wortlaut als Ausgangspunkt der Auslegung: Statt vieler *Henninger*, Europäisches Privatrecht und Methode, 2009, S. 280. Siehe hierzu bereits: Kap. 5, C., III., 1. *Divergierende Begriffe* und dort die Fn. 83.

<sup>63</sup> Französisch: „nécessaire“, Spanisch: „necesario“, Italienisch: „necessario“, Niederländisch: „noodzakelijk“.

<sup>64</sup> Französisch: „nécessaire“, Spanisch: „necesario“, Italienisch: „necessario“, Niederländisch: „noodzakelijk“.

Legt man dieses Wortverständnis zugrunde, erweckt es den Eindruck, der Gesetzgeber möchte die Grenze der Erforderlichkeit einer Datenverarbeitung bereits sehr früh ziehen. In seiner Rechtsprechung verweist der EuGH häufig darauf, dass die Einschränkungen des Datenschutzes auf das „*absolut Notwendige*“ begrenzt werden müssten.<sup>65</sup> Es verwundert daher auch nicht, wenn im Zusammenhang der Erforderlichkeit hierauf verwiesen wird.<sup>66</sup>

Keine Informationen gibt der Wortlaut der Regelung jedoch darüber, wie gut das Ziel erreicht werden soll bzw. darf. Zwar beschreibt der Begriff der Erforderlichkeit die zwingende Verbindung zwischen der Datenverarbeitung und dem verfolgten Zweck. Doch sobald man nach einem qualitativen Kriterium in der Hinsicht fragt, ob die Datenverarbeitung erforderlich sein muss, um den verfolgten Zweck gerade so zu erreichen oder aber besser zu erreichen, gibt der Wortlaut hierauf keine konkreten Antworten.<sup>67</sup> So ließe sich schließlich auch argumentieren, dass eine Datenverarbeitung erforderlich ist, um den verfolgten Zweck gut oder sogar bestmöglich zu erzielen. Diese Frage bildet der Wortlaut

---

<sup>65</sup> Siehe dies konkret zur Erforderlichkeit einer Datenverarbeitung im Rahmen von Rechtsgrundlagen: EuGH, Rs. C-13/16 (Rīgas satiksmē), ECLI:EU:C:2017:336 = BeckRS 2017, 108615, Rn. 30, zu Art. 7 lit. f) DS-RL; EuGH, Rs. C-708/18 (Asociația de Proprietari bloc M5A-ScaraA), ECLI:EU:C:2019:1064 = ZD 2020, S. 148, Rn. 46, zu Art. 7 lit. f) DS-RL. Siehe auch allgemein: EuGH, Rs. C-73/07 (Satakunnan Markkinapörssi und Satamedia), ECLI:EU:C:2008:727 = EuZW 2009, S. 108, Rn. 56; EuGH, Rs. C-439/19 (Latvijas Republikas Saeima ([Points de pénalité])), ECLI:EU:C:2021:504 = BeckRS 2021, 15289, Rn. 105, 110.

<sup>66</sup> Siehe Simitis/Hornung/Spiecker gen. Döhmman/Roßnagel, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 77, zu Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO; auch zur Erforderlichkeit nach Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO Kübling/Klar/Sackmann, Datenschutzrecht, 5. Aufl. 2021, Rn. 402; siehe hierzu auch Taeger/Gabel/Taeger, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DS-GVO, Rn. 94, ohne diesbezüglich ausdrücklich auf die Rechtsprechung des EuGH zu verweisen; Simitis/Hornung/Spiecker gen. Döhmman/Schantz, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 100, zur Erforderlichkeit nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO; siehe auch Moos/Schefzig/Arning/Arning, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 40, jedenfalls als zusätzlicher (Praxis-)Hinweis, ohne aber final hierzu Stellung zu beziehen.

<sup>67</sup> So wohl auch *Albers*, Informationelle Selbstbestimmung, 2005, S. 519, zwar zur Rechtslage vor der Datenschutz-Grundverordnung und wohl mit Fokus auf das nationale Grundrecht der informationellen Selbstbestimmung aber in diesem Zusammenhang wohl anhand des Begriffs Erforderlichkeit selbst; vgl. ebenfalls *Robrahn/Bremert*, ZD 2018, S. 291, 293, die darauf hinweisen, dass „Zwecke in einem unterschiedlichen Maß [...] erreicht werden können“.

nicht ab und kann daher nicht aus der Formulierung „*erforderlich*“ festgemacht werden.

## 2. Systematik

Die Systematik, nach der der Tatbestand der Erforderlichkeit als Bindeglied zwischen der Datenverarbeitung und dem Verarbeitungszweck fungiert, ist entscheidend für die Auslegung des Begriffs. Daher müssen in die Auslegung auch die Bezugspunkte des Tatbestands der Erforderlichkeit mit einbezogen werden. Es bedarf damit ebenfalls der Klärung, ob die Datenschutz-Grundverordnung eine qualitative Betrachtung der Bezugspunkte der Erforderlichkeit zulässt, die dann letztlich auf den Tatbestand der Erforderlichkeit selbst durchschlagen könnten.

Obwohl es hier um das systematische Zusammenspiel der Erforderlichkeit in ihrer Funktion als Verknüpfung der beiden Bezugspunkte handelt, kann eine systematische Auslegung hierauf keine Antworten geben. Dennoch ist es wichtig, auf diese Funktion hinzuweisen. Denn hierdurch verbietet sich eine isolierte Betrachtung des bloßen Begriffs der Erforderlichkeit.

## 3. Telos

Eine Antwort auf die Frage, ob die Datenschutz-Grundverordnung eine qualitative Betrachtung der Bezugspunkte im Rahmen der Erforderlichkeit zulässt, könnte sich allenfalls aus dem Telos ergeben.

Der Sinn und Zweck des Tatbestands liegt zunächst einmal in der Aufgabe, Datenverarbeitungen weiter einzuschränken.<sup>68</sup> Für eine enge Auslegung der Erforderlichkeit und damit weitgehende Einschränkung der Datenverarbeitung könnte die Aussage des EuGH gedeutet werden, wenn dieser eben darauf abstellt, dass die Einschränkungen des Schutzes auf das „*absolut Notwendige*“ zu beschränken sind.<sup>69</sup> Diese Aussage des EuGH erinnert gleichzeitig an das „*hohe Datenschutzniveau*“, das die Datenschutz-Grundverordnung ausweislich der

---

<sup>68</sup> Vgl. Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 2017, Rn. 429.

<sup>69</sup> Statt vieler: EuGH, Rs. C-13/16 (Rīgas satiksmē), ECLI:EU:C:2017:336 = BeckRS 2017, 108615, Rn. 30. Siehe hierzu: Kap. 10, D., II., 1. *Wortlaut* und dort die Fn. 65.

ErwG 6, 10, 13 DS-GVO als allgemeines Ziel zugrunde legt und auf das der EuGH allgemein in seinen Entscheidungen auch häufig abstellt.<sup>70</sup>

Ein solch pauschaler Verweis wäre als Argumentation für die Auslegung des Tatbestands der Erforderlichkeit allerdings lückenhaft. Zunächst ist auch hier wieder darauf hinzuweisen, dass sich allgemeine Ziele eines Rechtsakts nicht dazu eignen, die Auslegung einzelner Vorschriften dieses Rechtsakts zu bestimmen.<sup>71</sup> Selbst wenn die Datenschutz-Grundverordnung einen hohen Schutz der betroffenen Personen gewährleisten will, muss damit nicht zwangsweise jede Vorschrift der Datenschutz-Grundverordnung diesem „Anspruch“ genügen und daher stets streng zugunsten der betroffenen Person ausgelegt werden.

Zu beachten ist nämlich, dass die Datenschutz-Grundverordnung zwar auf der einen Seite den Schutz der betroffenen Person bei Verarbeitungen ihrer personenbezogenen Daten gewährleisten will. Gleichzeitig schafft die Datenschutz-Grundverordnung aber auch die Grundlage für Datenverarbeitungen unter Beachtung dieser Rechte. In ihrer Gesamtheit ist die Datenschutz-Grundverordnung daher der Ausdruck eines Kompromisses zwischen dem Schutz vor einer Verarbeitung und dem Interesse an einer Verarbeitung personenbezogener Daten.<sup>72</sup> Die Verordnung daher nachträglich nur im Licht eines dieser Ziele zu betrachten, wird ihr nicht gerecht.

---

<sup>70</sup> EuGH, Rs. C-507/17 (Google [Räumliche Reichweite der Auslistung]), ECLI:EU:C:2019:772 = NJW 2019, S. 3499, Rn. 54; EuGH, Rs. C-645/19 (Facebook Ireland u.a.), ECLI:EU:C:2021:483 = NJW 2021, S. 2495, Rn. 45; EuGH, Rs. C-579/21 (Pankki S), ECLI:EU:C:2023:501 = NZA 2023, S. 889, Rn. 55; EuGH, Rs. C-340/21 (Natsionalna agentsia za prihodite), ECLI:EU:C:2023:986 = BeckRS 2023, 35786, Rn. 73; EuGH, Rs. C-667/21 (Krankenversicherung Nordrhein), ECLI:EU:C:2023:1022 = BeckRS 2023, 36822, Rn. 98.

<sup>71</sup> Statt vieler Riesenhuber/*Riesenhuber*, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 42; siehe hierzu: Kap. 4, C., I. *Die Konkretisierung durch Art. 32 Abs. 2 DS-GVO* und dort insb. die Fn. 53.

<sup>72</sup> Siehe EuGH, Rs. C-667/21 (Krankenversicherung Nordrhein), ECLI:EU:C:2023:1022 = BeckRS 2023, 36822, Rn. 98, wobei der EuGH diesen Interessenausgleich schon deutlich vorprägt, indem er bei den auszugleichenden Positionen bereits zu Beginn von einem „*hobe[n] Schutzniveau*“ der betroffenen Personen ausgeht; Herfurth, ZD 2018, S. 514, 514, wonach „*[n]abezu allen Vorschriften der DS-GVO*“ dieser Interessenausgleich zugrunde liegt; ähnlich auch Simitis/Hornung/Spiecker gen. Döhmman/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 1 DS-GVO, Rn. 34, „*[...] dass die DSGVO [...] in ihren konkreten Regelungen bereits wesentliche Abwägungen mit [...] entgegenstehenden [...] Rechten integriert [...]*“; in diese Richtung auch Roßnagel, NJW 2019, S. 1, 3, konkret zur Frage der Rechtmäßigkeit

Die Aufgabe der Auslegung besteht daher vielmehr darin, die Funktionen einzelner Instrumente, Vorschriften, Tatbestände (etc.) in ihrem Gesamtgefüge zu betrachten und anhand dessen die spezifischen Ziele des Gesetzgebers zu ermitteln.<sup>73</sup> Wie bereits oben festgestellt wurde, liegt die Funktion der Erforderlichkeit nicht einfach nur in der Einschränkung einer Datenverarbeitung. Der Tatbestand dient als Ausgleich zwischen dem Schutzinteresse und dem Verarbeitungsinteresse. Ein Maßstab für die Auslegung der Erforderlichkeit sollte daher auch beide widerstreitenden Interessenlagen gebührend berücksichtigen.<sup>74</sup>

---

einer Datenverarbeitung. Siehe auch hinsichtlich eines Ausgleichs des Schutzes betroffener Personen und dem freien Datenverkehr (was letztlich eine Datenverarbeitung darstellt) als die wesentlichen Ziele nach Art. 1 DS-GVO: Hornung/Schallbruch/Jandt, IT-Sicherheitsrecht, 2021, § 17, Rn. 18, wonach die Vorschriften der Datenschutz-Grundverordnung als „*Essenz der Abwägung*“ hierzwischen anzusehen seien; in eine ähnlich Richtung Jandt/Steidle/Ambrock, Datenschutz im Internet, 2018, A. II., Rn. 44; siehe auch Freund u.a./Schmidt/Heinson, DSGVO, 2023, Art. 1 DS-GVO, Rn. 18; Franzen/Gallner/Oetker/Franzen, EuArbRK, 5. Aufl. 2024, 270. Datenschutz-Grundverordnung, Art. 1 DS-GVO, Rn. 2.

<sup>73</sup> Vgl. Riesenhuber/Riesenhuber, Europäische Methodenlehre, 4. Aufl. 2021, § 10, Rn. 42; siehe auch Wank, Juristische Methodenlehre, 2020, § 18, Rn. 96 ff., mit seiner Kritik am EuGH, die Zwecke nicht oder nicht ausreichend herauszuarbeiten.

<sup>74</sup> Siehe vereinzelt den Verweis auf eine Interessenabwägung im Rahmen der Erforderlichkeit: BeckOK Datenschutzrecht/Albers/Veit, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 19 f., aber wohl nur eingeschränkt; Däubler u.a./Wedde, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 8 f., verweist wohl auf eine Interessenabwägung, wenn es Alternativen zur Datenverarbeitung gibt, um die Erforderlichkeit zu bestimmen; Schlegel, ZD 2020, S. 243, 244, verlangt eine „*am Verhältnismäßigkeitsgrundsatz ausgerichtete Interessenabwägung*“ im Rahmen der Erforderlichkeit (allerdings nach der nationalen Regelung des § 26 Abs. 1. S. 1 BDSG und mit weiteren Nachweisen); im Ansatz auch Kühling/Buchner/Buchner/Petri, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 45 zu Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO und Rn. 119 zu lit. e), wobei letzteres wohl auf die grundrechtliche Verhältnismäßigkeitsprüfung abzielt; siehe auch Chibanguza/Kuß/Steegen/Steegen/Kuß, Künstliche Intelligenz, 2022, § 2, C., Rn. 42, die bei der Bestimmung der Erforderlichkeit im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO darauf abstellen, dass „*die beiderseitigen Interessen maßgeblich*“ sein sollen; Specker gen. Döhmann u.a./Sartor, GDPR, 2023, Art. 6 GDPR, Rn. 38, verlangt für Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO einen Ausgleich der Interessen, siehe auch Rn. 68 in Bezug auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO (aber wohl zurückhaltender); Wybitul/Pöiters/Rauer, Hdb. EU-Datenschutz-Grundverordnung, 2017, Art. 6 DS-GVO, Rn. 16, die für die Erforderlichkeit im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO eine „*Verhältnismäßigkeitsprüfung*“ anwenden wollen, bei der eine Interessenabwägung innerhalb einer „*abgeschwächten Angemessenheitsprüfung*“ zu erfolgen hat; siehe auch zu Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO Schuster/Grützmacher/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-



Um einem solchen Ausgleich gerecht werden zu können, müssen beide Bezugspunkte, also die Datenverarbeitung mit ihrem dahinterstehenden Interesse am Schutz vor einer Verarbeitung und dem Zweck der Verarbeitung als Ausdruck des Interesses an der Verarbeitung, auch qualitativ in die Bewertung mit aufgenommen werden. Zugunsten des Verarbeitungsinteresses sollte daher ebenfalls berücksichtigt werden, in welcher Qualität die Datenverarbeitung den Zweck der Verarbeitung erfüllt.

### III. Würdigung der Bewertungsmaßstäbe und eigene Lösung

Die Auslegung des Tatbestands hat gezeigt, dass der dritte, vorgestellte Bewertungsmaßstab von der richtigen Grundannahme ausgeht und das Verhältnis der Datenverarbeitung und ihren Zweck in den Vordergrund stellt. Hierbei handelt es sich um nichts anderes als um eine Abwägung der, hinter den beiden Bezugspunkten des Tatbestands stehenden Interessen. Dies dürfte wohl auch von den Vertretern des dritten Bewertungsmaßstabs in gewissem Maße geteilt werden, wenn diese gerade darauf abstellen, dass mit dieser Bewertung eine „Bandbreite“ verbunden ist, in dessen Rahmen unterschiedliche Interessen berücksichtigt werden können.<sup>75</sup> Der Tatbestand der Erforderlichkeit soll somit einen Ausgleich zwischen der Datenverarbeitung und dem Erreichen des Verarbeitungszwecks schaffen.

Problematisch hieran ist die damit verbundene Abstraktheit der Bewertung, wann eine Datenverarbeitung als erforderlich anzusehen ist. Denn im Endeffekt wird damit auf den Einzelfall verwiesen. Für eine praktische Umsetzung dieser Abwägung sollte man daher nicht die beiden anderen Bewertungsmaßstäbe außer Acht lassen. Denn bei einer genaueren Betrachtung dieser Ansätze, handelt

---

Grundverordnung, Art. 6 DS-GVO, Rn. 27, aber später bei der Erforderlichkeit nach Art. 6 Abs. 1 UAbs. 1 lit. c) DS-GVO gegen eine Interessenabwägung ist (Rn. 33). Gegen eine Interessenabwägung im Rahmen der Erforderlichkeit: Freund u.a./Schmidt, DSGVO, 2023, Art. 6 DS-GVO, Rn. 54; Sydow/Marsch/Reimer, DS-GVO – BDSG, 3. Aufl. 2022, Art. 6 DS-GVO, Rn. 27, gegen eine Interessenabwägung im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO; auch gegen eine Interessenabwägung im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO Feiler/Forgó, EU-DSGVO und DSG, 2. Aufl. 2022, Art. 6 DS-GVO, Rn. 9; Gierschmann u.a./Assion/Nolte/Veil, Datenschutz-Grundverordnung, 2018, Art. 6 DS-GVO, Rn. 88, die eine „allgemeine Güterabwägung“ im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO ablehnen.

<sup>75</sup> BeckOK Datenschutzrecht/Albers/Veil, Stand: 46. Ed. 2023, Art. 6 DS-GVO (Stand: August 2023), Rn. 19.

es sich bei ihnen um nichts anderes als eine vordefinierte Verkörperung (von Teilen) dieser Interessenabwägung.

So zielt die Suche nach möglichen Alternativen zur Datenverarbeitung darauf ab, dem Interesse am Schutz vor einer Verarbeitung stärkeres Gewicht zu verschaffen, aber gleichzeitig das Interesse an der Verarbeitung und ihrem Zweck anzuerkennen. Ähnliches zeigt sich auch bei dem zweiten Bewertungsansatz, wenn dort durch eine Differenzierung in der Qualität der Zweckerreichung dem Verarbeitungsinteresse unterschiedlich starkes Gewicht zugesprochen wird. Dass es sich bei den anderen Bewertungsansätzen um eine Ausformung der Interessenabwägung handelt, dürfte dabei am deutlichsten aus der Kombination beider Ansätze erkennbar werden, wenn man die Erforderlichkeit daran bemisst, dass es keine zumutbaren Alternativen gibt, um den Zweck effektiv zu erreichen. Denn hier werden gerade beide Interessen einander gegenübergestellt. Zum anderen wird mit dem Erfordernis der „Zumutbarkeit“ von Alternativen gerade ein abwägendes Kriterium verlangt, dass wohl ebenfalls daran zu beurteilen sein dürfte, welchem Interesse im konkreten Einzelfall hier der Vorzug zu gewähren ist.<sup>76</sup>

Für die praktische Umsetzung kann es daher hilfreich sein, sich an den beiden erstgenannten Ansätzen zu orientieren, um den Ausgleich der Interessen vorzunehmen. So sollte die Erforderlichkeit dann anzunehmen sein, wenn es keine zumutbaren Alternativen gibt, um den Zweck der Verarbeitung effektiv zu erreichen. Hierin dürfte ein guter Ausgangspunkt liegen, um ein angemessenes Verhältnis zwischen den widerstreitenden Interessen zu erreichen. Zum einen wird hier auf die effektive und nicht irgendeine Erreichung des Zwecks aber auch nicht darüber hinaus abgestellt. Damit wird dem Verarbeitungsinteresse grds. eine solide Position in der Abwägung eingeräumt. Weiterhin sollte auch nicht bereits jede Alternative zur Datenverarbeitung ausreichen, die Erforder-

---

<sup>76</sup> Siehe Kühling/Buchner/*Buchner/Petri*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 6 DS-GVO, Rn. 45, konkret im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO; in diese Richtung lässt sich auch Däubler u.a./*Wedde*, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 6 DS-GVO, Rn. 9 verstehen, der bei Alternativen auf eine Interessenabwägung verweist und später auch die Zumutbarkeit erwähnt. Siehe auch Simitis/Hornung/Spiecker gen. Döhmman/*Schantz*, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO, Rn. 32, im Zusammenhang des Art. 6 Abs. 1 UAbs. 1 lit. b) DS-GVO, aber ablehnend ggü. dem Maßstab der Zumutbarkeit. Vgl. hier auch die Kriterien für die Zumutbarkeit von Moos/Schefzig/*Arning/Arning*, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 5, Rn. 43.

lichkeit auszuschließen. Indem dabei auf die Zumutbarkeit der Alternativen abgestellt wird, wird die Bewertung um die wichtige, abwägende Komponente ergänzt. Hiermit lassen sich dann die Besonderheiten des Einzelfalls berücksichtigen.

Da es sich bei diesem Vorschlag eben nicht um einen festen Bewertungsansatz handelt, sondern eben um eine – für die Praxis – unterstützende Ausformung der eigentlich angedachten Interessenabwägung, kann bei atypischen Fällen, mit denen sich hier keine gerechten Ergebnisse erzielen lassen, wieder auf die allgemeine Interessenabwägung zurückgegriffen werden.

#### *IV. Zwischenergebnis*

Für die inhaltliche Auslegung des Tatbestands der Erforderlichkeit kommen mehrere Bewertungsmaßstäbe in Betracht, die das Verhältnis zwischen dem Eingriff in die Rechte der betroffenen Personen und dem Interesse an einer Verarbeitung unterschiedlich abbilden.

Im Rahmen der Auslegung des Tatbestands der Erforderlichkeit ist vor allem seine Funktion als Bindeglied zwischen der Datenverarbeitung und dem Zweck der Verarbeitung zu berücksichtigen. Die Besonderheiten, die sich aus diesem System ergeben können, werden vom Wortlaut nicht umfänglich abgebildet. Die Auslegung darf daher aber nicht an dem Begriff selbst aufhören. Vielmehr müssen vor allem auch die beiden Bezugspunkt des Tatbestands bei der Auslegung berücksichtigt werden.

Im Endeffekt dient der Tatbestand der Erforderlichkeit dem Ausgleich zwischen der Datenverarbeitung und dem Zweck der Verarbeitung. Damit kommt es hier zu einem Ausgleich der dahinterstehenden Interessen. In der Praxis ist ein solcher Interessenausgleich aufgrund seiner Abstraktheit mit erheblichen Unsicherheiten verbunden. Daher kann es hilfreich sein, sich daran zu orientieren, dass von der Erforderlichkeit einer Datenverarbeitung auszugehen ist, wenn es zu ihr keine zumutbaren Alternativen gibt, den Zweck effektiv zu erreichen.

### E. Folgen für das Problem datenverarbeitender TOM

Aus dem Tatbestand der Erforderlichkeit erwachsen mehrere Probleme für das Spannungsverhältnis.

### *I. Einschränkung der weiteren Untersuchung*

Der Tatbestand der Erforderlichkeit dient als Bindeglied zwischen der Datenverarbeitung und dem Zweck der Verarbeitung. Die Entscheidung darüber, ob eine Datenverarbeitung im Rahmen datenverarbeitender TOM datenschutzrechtlich zulässig ist, entscheidet sich daher am Einzelfall. Wie bereits einleitend in dieser Arbeit herausgestellt wurde, sollen einzelne TOM nicht behandelt werden.<sup>77</sup> Damit ist es auch nicht möglich, eine abschließende Entscheidung über die datenschutzrechtliche Zulässigkeit von datenverarbeitenden TOM zu geben.

In den Vordergrund müssen daher die Bewertungsmaßstäbe rücken, die, auf den Einzelfall angewandt, letztlich über die Rechtmäßigkeit der Verarbeitung und damit auch über die zulässige Implementierung datenverarbeitender TOM entscheiden.

### *II. Wechselwirkung zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle*

Ein wesentliches Problem für die Lösung datenverarbeitender TOM ist jedoch die Entstehung einer Wechselwirkung zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Rechtmäßigkeit datenverarbeitender TOM. Nach den Ergebnissen des 2. Teils lassen sich die datenschutzrechtlichen Anforderungen an die technischen und organisatorischen Maßnahmen im Rahmen der Sicherheit der Verarbeitung berücksichtigen.<sup>78</sup> Die Untersuchung der datenschutzrechtlichen Anforderungen an die datenverarbeitenden TOM hat jedoch gezeigt, dass die Entscheidung über ihre Rechtmäßigkeit erheblich von dem Zweck abhängt, der mit der Datenverarbeitung und damit mit den datenverarbeitenden TOM verfolgt wird.<sup>79</sup>

Für datenverarbeitende TOM liegt der Zweck wiederum in der konkreten Gewährleistung der Sicherheit der jeweiligen Verarbeitung.<sup>80</sup> Damit beeinträchtigt die Rechtmäßigkeit der Datenverarbeitung im Rahmen der TOM nicht nur

---

<sup>77</sup> Siehe hierzu: Kap. 3, C., I. *Betrachtung des Gesamtproblems.*

<sup>78</sup> Siehe hierzu: Kap. 7, D. *Zwischenergebnis.*

<sup>79</sup> Siehe hierzu: Kap. 8, B. *Ausrichtung am Zweck der Verarbeitung* und Kap. 10, B., III. *Der Zweck als zweiter Bezugspunkt.*

<sup>80</sup> Siehe hierzu: Kap. 9, A. *Die Sicherheit der Verarbeitung als Verarbeitungszweck?.*

die Anforderungen an die Sicherheit der Verarbeitung. Die Sicherheit der Verarbeitung beeinflusst wiederum auch die Entscheidung über die datenschutzrechtliche Rechtmäßigkeit der Verarbeitung.

### *III. Der Auslegungsmaßstab der Erforderlichkeit als entscheidende Weichenstellung*

Die Sicherheit der Verarbeitung beeinflusst die datenschutzrechtliche Rechtmäßigkeit vorrangig auf der Ebene des Tatbestands der Erforderlichkeit. Sie ist Ausdruck des Interesses an der Verarbeitung und muss daher im Rahmen der Erforderlichkeit ins Verhältnis zur Datenverarbeitung gesetzt werden.<sup>81</sup> Die Auslegung des Tatbestands der Erforderlichkeit hat damit eine besondere Bedeutung für die Rechtmäßigkeit der Datenverarbeitung im Allgemeinen und damit auch für die hier untersuchten Fälle. Denn abhängig davon, wie streng die Erforderlichkeit ausgelegt wird, hat dies wiederum Auswirkungen auf das Problem datenverarbeitender TOM im Rahmen der Sicherheit der Verarbeitung.

Je strenger die Anforderungen an die Erforderlichkeit sind, desto eher scheitert eine Rechtmäßigkeit der Verarbeitung und für datenverarbeitende TOM bedeutet dies, dass sie datenschutzrechtlich gesehen nicht implementiert werden dürfen. Im Lichte der Sicherheit der Verarbeitung hätte das nun wieder zur Folge, dass über eine Absenkung der Sicherheit der Verarbeitung nachgedacht werden muss, wenn die dadurch entstehende Lücke nicht unter Berücksichtigung der Abwägungskriterien des Art. 32 Abs. 1 DS-GVO verhältnismäßig geschlossen werden kann.

Über die Auswirkungen des Tatbestands der Erforderlichkeit auf die Sicherheit der Verarbeitung sollte man sich bewusst sein, denn hierin liegt ein wesentlicher Punkt, den es bei der Erarbeitung eines Lösungsvorschlags zu beachten gilt. Nach der hier vertretenen Ansicht ist die Erforderlichkeit anhand einer Interessenabwägung zu bestimmen, die einen Ausgleich zwischen der Erreichung des Zwecks und dem damit verfolgten Interesse an der Verarbeitung und der Datenverarbeitung und dem bedingten Eingriff in das Schutzinteresse schaffen soll. Bei der praktischen Umsetzung kann die Suche nach zumutbaren Alternativen zur effektiven Erreichung des Zwecks die Abwägung erleichtern.

---

<sup>81</sup> Siehe hierzu: Kap. 10, D., III. *Würdigung der Bewertungsmaßstäbe und eigene Lösung.*



## Teil 4

Lösungsvorschlag für das Spannungsverhältnis





## Kapitel 11

# Methodik

### A. Untersuchungsergebnisse als Basis für den Lösungsansatz

Die Untersuchung hat gezeigt, dass das vermutete Spannungsverhältnis zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle im Falle datenverarbeitender TOM tatsächlich besteht und einer Lösung bedarf.<sup>1</sup> Obwohl Art. 32 DS-GVO zur Gewährleistung der Sicherheit der Verarbeitung keine Pflicht zur Implementierung konkreter TOM vorsieht und somit auch keine unmittelbare Pflicht zur Implementierung datenverarbeitender TOM besteht, beeinflussen rechtliche Hindernisse die Umsetzung der Sicherheit der Verarbeitung.<sup>2</sup> Daher müssen sie auch bereits bei der Festlegung des geforderten Schutzniveaus im Zusammenhang der Angemessenheitsprüfung berücksichtigt werden.<sup>3</sup> Eine Subsumtion unter die genannten Abwägungskriterien der Angemessenheit scheidet hier aus.<sup>4</sup> Die datenschutzrechtliche Bewertung von TOM ist allerdings als ungeschriebenes Tatbestandsmerkmal Teil dieser Prüfung.<sup>5</sup>

Bei datenverarbeitenden TOM erfolgt die datenschutzrechtliche Bewertung anhand der datenschutzrechtlichen Vorabkontrolle i.S.d. Art. 6 DS-GVO. Es bedarf somit einer Rechtsgrundlage für die, den Maßnahmen zugrundeliegende Datenverarbeitung.<sup>6</sup> Eine rechtssichere Grundlage für die Gewährleistung der

---

<sup>1</sup> Siehe hierzu: Kap. 2, A. *Begründung eines Spannungsverhältnisses zwischen Art. 32 und Art. 6 DS-GVO* und Kap. 6, C. *Überarbeitung der Arbeitshypothese*.

<sup>2</sup> Siehe hierzu: Kap. 6, C. *Überarbeitung der Arbeitshypothese*.

<sup>3</sup> Siehe hierzu: Kap. 7, A. *Überlegungen zur Berücksichtigung datenverarbeitender TOM*.

<sup>4</sup> Siehe hierzu: Kap. 7, B. *Subsumtion unter die Abwägungskriterien des Art. 32 Abs. 1 DS-GVO*.

<sup>5</sup> Siehe hierzu: Kap. 7, C. *Die datenschutzrechtliche Bewertung von TOM als ungeschriebenes Tatbestandsmerkmal der Abwägung*.

<sup>6</sup> Siehe hierzu: Kap. 2, A., II. *Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO* und Kap. 8, A. *Die Notwendigkeit einer Rechtsgrundlage*.

Sicherheit der Verarbeitung i.S.d. Art. 32 DS-GVO kann dabei nur durch die gesetzlichen Rechtsgrundlagen sichergestellt werden.<sup>7</sup> Welche dieser Rechtsgrundlagen letztlich einschlägig ist, kann erstmal dahinstehen und anhand des Einzelfalls entschieden werden.<sup>8</sup> Vorrangig von Bedeutung ist hingegen der gemeinsame Tatbestand der Erforderlichkeit. Der Tatbestand dient als Kontrolle vor überschießenden Datenverarbeitungen, indem er diese ins Verhältnis zum verfolgten Zweck der Verarbeitung setzt und sicherstellt, dass die Datenverarbeitung erforderlich ist, um den Zweck zu erreichen.<sup>9</sup> Dahinter steht die Abwägung der Interessen am Schutz der betroffenen Person vor einer Verarbeitung und das Interesse an der Verarbeitung.

Mit Blick auf die datenschutzrechtliche Bewertung datenverarbeitender TOM und deren Auswirkungen auf die Anforderungen an die Sicherheit der Verarbeitung kommt es dabei zu einer Wechselwirkung.<sup>10</sup> Denn nicht nur die rechtliche Bewertung datenverarbeitender TOM beeinflusst die Sicherheit der Verarbeitung, indem sie im Rahmen der Angemessenheit des Schutzniveaus zu berücksichtigen ist. Die Bestimmung der Rechtmäßigkeit datenverarbeitender TOM ist durch den Verarbeitungszweck im Rahmen des Tatbestands der Erforderlichkeit wiederum anhand der Gewährleistung der Sicherheit der Verarbeitung zu bemessen.

Damit beeinflussen sich beide Bereiche gegenseitig. Hierdurch wird nicht nur das Spannungsverhältnis verkompliziert. Auch ein Lösungsansatz muss dieser Wechselwirkung gebührend Rechnung tragen.

---

<sup>7</sup> Siehe hierzu: Kap. 9, C. *Die Frage einschlägiger Rechtsgrundlagen.*

<sup>8</sup> Siehe hierzu: Kap. 9, C., II. *Schlussfolgerungen und denkbare Rechtsgrundlagen für datenverarbeitende TOM.*

<sup>9</sup> Siehe hierzu: Kap. 10, A. *Der Tatbestand im System der Rechtsgrundlagen* und B. *Bezugspunkte des Tatbestands.*

<sup>10</sup> Siehe hierzu: Kap. 10, E., II. *Wechselwirkung zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle.*

## B. Ansatz zur Lösung des Spannungsverhältnisses

### *I. Grundlage*

Im 1. Teil wurden drei denkbare Lösungsansätze vorgestellt, mit denen man das Spannungsverhältnis begegnen könnte.<sup>11</sup> Die ersten zwei Vorschläge priorisieren entweder die Sicherheit der Verarbeitung oder die datenschutzrechtliche Vorabkontrolle und geben diesen Regelungen den Vorrang vor der jeweils anderen. Aufgrund der Ergebnisse des 2. und 3. Teils und vor allem der festgestellten Wechselwirkung erscheint ein solcher Vorrang eines Regelungsbereichs vor den anderen kein angemessener Ansatz zu sein, um das Problem zu lösen.

Gerechter wäre es daher zu versuchen, im Wege des 3. Lösungsansatzes den Wertungen beider Regelungsbereiche Rechnung zu tragen und beide Bereiche i.S.e. „praktischen Konkordanz“ miteinander auszugleichen. Aufgrund der starken Verflechtung dürfte jedoch eine gleichwertige Berücksichtigung nicht möglich sein. Vielmehr müsste man zunächst die Wechselwirkung durchbrechen, um einen Punkt zu finden, an dem man ansetzen kann. Dabei ist allerdings zu beachten, einen solchen Punkt zu finden, der nicht bereits zu Beginn den angestrebten Ausgleich zwischen beiden Bereichen zu stark einseitig beeinflusst.

### *II. Instrumente*

Ein Ausgleich beider Rechtsbereiche setzt zunächst voraus, dass beide Bereiche über die entsprechenden Instrumente verfügen, einen solchen Ausgleich (de lege lata) rechtlich abzubilden. Die (methodischen) Instrumente für die Sicherheit der Verarbeitung und für die datenschutzrechtliche Vorabkontrolle wurden jeweils im 2. und 3. Teil erarbeitet.

Für die Sicherheit der Verarbeitung ist es das Angemessenheitskriterium der datenschutzrechtlichen Bewertung von TOM und für die datenschutzrechtliche Vorabkontrolle ist es der Tatbestand der Erforderlichkeit. Beide Tatbestände erlauben die Berücksichtigung der Wertungen des jeweils anderen Bereichs. So können rechtliche Bedenken gegen eine Datenverarbeitung im Rahmen datenverarbeitender TOM, die Teil der datenschutzrechtlichen Vorabkontrolle sind, durch den Abwägungstatbestand der datenschutzrechtlichen Bewertung zu einer Absenkung der Sicherheit der Verarbeitung führen.<sup>12</sup>

---

<sup>11</sup> Siehe hierzu: Kap. 3, A. *Probleme und Ziele der Arbeit*.

<sup>12</sup> Siehe hierzu: Kap. 7, D. *Zwischenergebnis*.

Datenverarbeiter werden insofern von der (faktischen) Pflicht befreit, datenschutzrechtlich bedenkliche Maßnahmen zu implementieren. Dagegen ist für die Erforderlichkeit der Datenverarbeitung datenverarbeitender TOM zu beachten, diese in das Verhältnis mit dem, der Datenverarbeitung verfolgten Zweck zu setzen und hier einen Ausgleich mit den dahinterstehenden Interessen zu erreichen. Als praktische Hilfe kann hierbei Beachtung finden, ob der Zweck nicht mit zumutbaren Alternativen ebenfalls effektiv erreicht werden kann.<sup>13</sup>

Ein Ausgleich beider Rechtsbereiche könnte daher auf der Ebene der jeweiligen Tatbestände stattfinden. Besonders auffällig ist hierbei, dass es sich bei beiden Instrumenten um Abwägungstatbestände handelt. Hierin liegt sowohl eine Chance als auch eine Herausforderung in der Formulierung eines Lösungsvorschlags. Abwägungstatbeständen ist, anders als „statischen“ Tatbeständen, eine Offenheit immanent, die es erlaubt, über ihre (vermeintlichen) Grenzen hinaus, den Ausgleich der hier bestehenden Interessen zu ermöglichen. Gleichzeitig erschwert dies aber auch die spätere, praktische Umsetzung. Denn eine Abwägung ist stets mit Rechtsunsicherheiten verbunden.

### *III. Ziele eines Lösungsansatzes*

#### *1. Allgemeines*

Ein gerechter Ansatz für die Lösung des Spannungsverhältnisses im Rahmen datenverarbeitender TOM liegt in einem Ausgleich der widerstreitenden Vorschriften. Beide Regelungsbereiche verfügen auch über die notwendigen Instrumente, einen solchen Ausgleich zu erreichen. Bevor ein solcher Lösungsvorschlag allerdings formuliert werden kann, sollte man sich noch über die Ziele klar werden, die mit dieser Lösung erreicht werden sollen. Denn es geht nicht einfach nur darum, die Vorschriften miteinander auszugleichen. Der Fokus muss darin liegen, einen „Misstand“ zu beheben. Ein Lösungsansatz sollte daher zielorientiert ausgestaltet sein, damit das eigentliche Problem auch gelöst werden kann.

Bereits im 2. Teil wurden die Folgen des Spannungsverhältnisses aus dem 1. Teil näher konkretisiert.<sup>14</sup> Es gibt zwar keine unmittelbare Verpflichtung be-

<sup>13</sup> Siehe hierzu: Kap. 10, D., III. *Würdigung der Bewertungsmaßstäbe und eigene Lösung.*

<sup>14</sup> Siehe hierzu: Kap. 6, C. *Überarbeitung der Arbeitshypothese.*

stimmte TOM zu implementieren, wodurch Datenverarbeiter auch nicht unmittelbar vor das Risiko gestellt werden, dass die Implementierung dieser Maßnahmen an anderer Stelle der Rechtsordnung verboten sein könnten. Die rechtlichen Probleme datenverarbeitender TOM wirken sich allerdings auf das Gebot der Verhältnismäßigkeit aus, dass der Pflicht zur Gewährleistung der Sicherheit der Verarbeitung zugrunde liegt.

Um diesem Gebot über die Grenzen des Art. 32 DS-GVO Geltung zu verschaffen, stehen zwei Stellschrauben zur Verfügung. Entweder ist im Rahmen des Art. 32 DS-GVO das Schutzniveau zu reduzieren, womit es dann schon von Beginn an nicht angemessen wäre, datenschutzrechtlich bedenkliche TOM zu implementieren. Alternativ könnte man auf Seiten der fraglichen TOM die Datenverarbeitung für rechtmäßig erklären und damit die rechtlichen Bedenken abbauen. Geht man von diesem Gedanken aus, muss ein Lösungsansatz, der auf einen Ausgleich der widerstreitenden Vorschriften abzielt, die Frage beantworten, wann eine Absenkung des Schutzniveaus gerechter ist und wann man die Datenverarbeitung von datenverarbeitenden TOM für rechtmäßig erklären muss.

## 2. Die Bedeutung alternativer TOM

Als Maßstab für die Entscheidung, in welchen Fällen es gerechter ist, der einen oder der anderen Vorschrift Geltung zu verschaffen und damit insgesamt einen Ausgleich zwischen beiden Vorschriften zu gewährleisten, könnte anhand des Bestehens alternativer TOM entschieden werden. Denn innerhalb des Spannungsverhältnisses kommen alternativen TOM eine besondere Bedeutung zu.

Auf der Seite der Sicherheit der Verarbeitung müssen für das geforderte Schutzniveau das Risiko und der Aufwand, dieses Risiko auszugleichen, in Relation zueinander gesetzt werden (Zweck-Mittel-Relation).<sup>15</sup> Welcher Aufwand besteht, richtet sich nach einer Bewertung der technischen und organisatorischen Maßnahmen anhand der (mindestens) drei Kriterien „Stand der Technik“, „Implementierungskosten“ und „datenschutzrechtliche Bewertung“. Zu einem unverhältnismäßigen Aufwand und damit zu einer Absenkung des geforderten Schutzniveaus käme es, wenn diese Kriterien einzeln oder in ihrer Summe im Verhältnis zum Risiko nicht verhältnismäßig wären. Da diese Kriterien sich erstmal auf den Aufwand zur Implementierung der Sicherheit der Verarbeitung

---

<sup>15</sup> Siehe hierzu: Kap. 7, B., V. *Systematisierung und Zwischenergebnis*.

insgesamt (also alle TOM gemeinsam) bezieht, kann die Unverhältnismäßigkeit einzelner Maßnahmen nicht unmittelbar zur Absenkung der gesamten Sicherheit führen.<sup>16</sup> Im Lichte einzelner (datenverarbeitender) TOM kommt es daher erstmal darauf an, welche alternativen TOM bestehen und ob deren Implementierung verhältnismäßig ist. Nur dort wo keine Alternativen bestehen, ist die Verhältnismäßigkeit direkt anhand der einzelnen TOM und damit im direkten Vergleich zum Risiko zu bestimmen.

Auf Seiten der datenschutzrechtlichen Vorabkontrolle bemisst sich die Rechtmäßigkeit der Datenverarbeitung vorrangig an dem Tatbestand der Erforderlichkeit. Der Tatbestand der Erforderlichkeit soll einen Ausgleich zwischen der Datenverarbeitung und dem verfolgten Zweck schaffen.<sup>17</sup> Für die praktische Umsetzung kommt dabei aber den Alternativen zu einer Datenverarbeitung eine entscheidende Bedeutung zu. Denn eine Abwägung der Interessen kann sich praxisgerecht daran orientieren, ob ein Ausweichen auf diese Alternativen für den Verantwortlichen zumutbar ist, um den Verarbeitungszweck effektiv zu erreichen.<sup>18</sup> Gibt es zumutbare Alternativen zur Datenverarbeitung, dann spricht dies dafür, dass die Verarbeitung nicht erforderlich ist. Übertragen auf den Untersuchungsgegenstand bedeutet dies: Können also andere TOM das Schutzniveau ebenfalls auf zumutbare Weise erreichen, dann ist die Datenverarbeitung im Rahmen der datenverarbeitenden TOM nicht erforderlich und somit nicht rechtmäßig.

Es zeigt sich, dass die Wertungen beider Regelungsbereiche mit den alternativen TOM an einen gemeinsamen Punkt anknüpfen. Dies könnte dabei helfen, das Spannungsverhältnis aufzulösen, indem man versucht, die beiden Wertungen miteinander zu verbinden.

### 3. Zwischenergebnis

Der gewählte Lösungsansatz versucht die Wertungen beider Regelungen gleichsam zu berücksichtigen, um einen gerechten Kompromiss zu finden. Ziel des Lösungsansatzes muss es sein, das Gebot der Verhältnismäßigkeit im Rahmen

---

<sup>16</sup> Siehe hierzu: Kap. 7, A., I. *Zwingende Differenzierung zwischen Sicherheit und Sicherheitsmaßnahmen* und II. *Datenverarbeitende TOM als Teil der Angemessenheitsprüfung*.

<sup>17</sup> Siehe hierzu: Kap. 10, D., III. *Würdigung der Bewertungsmaßstäbe und eigene Lösung*.

<sup>18</sup> Siehe hierzu: Kap. 10, D., III. *Würdigung der Bewertungsmaßstäbe und eigene Lösung*.

der Sicherheit der Verarbeitung aufrechtzuerhalten. Wann eine Verletzung dieses Gebots droht, kann insbesondere anhand alternativer TOM festgemacht werden. Denn diese wirken sich sowohl auf Seiten der Sicherheit der Verarbeitung als auch auf Seiten der datenschutzrechtlichen Vorabkontrolle aus. Sie bilden damit eine Verknüpfung, die genutzt werden kann, die Wertungen beider Bereiche in Einklang zu bringen.

### C. Praktische Umsetzung des Lösungsansatzes

Zur Umsetzung des hier gewählten Lösungsansatzes bietet sich ein Prüfungsschema an, mit dem sich das Spannungsverhältnis lösen lässt. Der Ausgangspunkt sollte dabei die Sicherheit der Verarbeitung sein. Dieser Ausgangspunkt rechtfertigt sich schon aus rein logischen Erwägungen. Denn erst die Anforderungen an die Sicherheit der Verarbeitung begründen überhaupt das Spannungsverhältnis mit der datenschutzrechtlichen Vorabkontrolle. Nur wenn im Rahmen der Prüfung der Anforderungen datenverarbeitende TOM identifiziert und in Betracht gezogen werden, um die Sicherheit der Verarbeitung zu gewährleisten, stellt sich die Frage, wie das dadurch entstehende Spannungsverhältnis gelöst werden kann. Um das angemessene Schutzniveau für die Sicherheit der Verarbeitung bestimmen zu können, ist es zum einen erforderlich, das Risiko der Verarbeitung zu bestimmen. Ferner und hier relevanter bedarf es aber auch eines Überblicks über die zur Verfügung stehenden TOM, die in Abhängigkeit des Risikos die Sicherheit gewährleisten können.

An dieser Stelle der Anforderungsprüfung an die Sicherheit der Verarbeitung kann die Lösung ansetzen. Denn bei der Identifikation verfügbarer TOM lässt sich nicht nur identifizieren, ob datenverarbeitende TOM bestehen, die das Spannungsverhältnis begründen können. Ferner müssen auch alternative TOM untersucht werden, um hieraus die Angemessenheit des Schutzniveaus ableiten zu können. Die Angemessenheit des Schutzniveaus richtet sich dabei nach dem Aufwand zur Umsetzung der Sicherheit, der in Relation zum ermittelten Risiko der Verarbeitung zu setzen ist. Der Aufwand wiederum richtet sich nach den Abwägungskriterien und damit insbesondere nach dem Kriterium der datenschutzrechtlichen Bewertung.

Im Rahmen dieses Kriteriums müssen dann die Wertungen aus der datenschutzrechtlichen Vorabkontrolle berücksichtigt werden. Gleichzeitig setzt die

Wechselwirkung zwischen beiden Vorschriften ein. Um hier zu einer Lösung zu kommen, muss diese Wechselwirkung „durchbrochen“ werden. Zur Bestimmung, welches Schutzniveau für die Verarbeitung angemessen ist und demnach welche TOM zu implementieren sind, sollte man die Wertungen der datenschutzrechtlichen Vorabkontrolle direkt in die Angemessenheitsprüfung der Sicherheit der Verarbeitung integrieren, indem man die datenverarbeitenden TOM und ihre datenschutzrechtliche Bewertung mit den alternativen TOM vergleicht.

Wie nachfolgend im Detail zu zeigen ist, müssen hierbei Vereinfachungen vorgenommen werden, um diese Wechselwirkung zu durchbrechen, da eine abschließende rechtliche Bewertung der datenverarbeitenden TOM nur möglich wäre, wenn auch die Anforderungen an die Sicherheit der Verarbeitung bereits abschließend bestimmt wären. Dennoch lassen sich bereits ohne diese die rechtlichen Bedenken an die datenverarbeitenden TOM aufgrund ihrer Datenverarbeitung berücksichtigen. Ziel muss dabei sein, die Maßnahmen zu identifizieren, die zumutbar sind, um ein angemessenes Schutzniveau zu gewährleisten, ohne gleichzeitig zu stark in die datenschutzrechtlich geschützten Interessen der von den Maßnahmen betroffenen Personen einzugreifen.



## Kapitel 12

# Prüfungsablauf

Nachfolgend wird der Prüfungsablauf zur Bestimmung des angemessenen Schutzniveaus i.S.d. Art. 32 DS-GVO unter besonderer Berücksichtigung des Spannungsverhältnisses bei datenverarbeitenden TOM und dessen Auflösung dargestellt.

### A. Identifikation und Bewertung des Risikos der Verarbeitung

Ausgangspunkt für die Bestimmung des angemessenen Schutzniveaus ist die Bewertung des Risikos der Verarbeitung durch die Gefahren eines personal data breach.<sup>1</sup> Die Risikobewertung ist ein allgemeines Problem im Rahmen des Art. 32 DS-GVO und kann die Datenverarbeiter in der praktischen Umsetzung vor große Herausforderungen stellen. Da es sich hierbei aber nicht um ein spezifisches Problem handelt, das durch den Untersuchungsgegenstand begründet wird, sollen die Ausführungen hier nur allgemein erfolgen. Nachfolgend soll daher nur auf einige Tipps eingegangen werden, mit denen sich die Bewertung wohlmöglich vereinfachen ließe.

Der Maßstab für die Risikobewertung ist grundlegend das Risiko für die Rechte und Freiheiten der betroffenen Person. Der Begriff ist allerdings sehr abstrakt und könnte in der praktischen Umsetzung dazu führen, dass wesentliche Risiken außer Acht gelassen werden könnten. Es wird daher vorgeschlagen, dass sich die Risikobewertung nicht anhand des Schutzguts orientieren sollte, sondern anhand der Gefahren für das Schutzgut.<sup>2</sup> Mit der Sicherheit der Verarbeitung sollen die Gefahren eines personal data breach i.S.d. Art. 4 Nr. 12 DS-

---

<sup>1</sup> Siehe hierzu: Kap. 5, A. *Risikobewertung*.

<sup>2</sup> Siehe wohl mit Parallelen den Vorschlag von *Wennemann*, DuD 2018, S. 174, 176 f., der ausgehend von der jeweiligen „*Verarbeitungstätigkeit*“ (hierzu sogleich) die Anforderungen aus

GVO verhindert oder wenigstens minimiert werden,<sup>3</sup> um im Endeffekt vor einem Risiko für die Rechte und Freiheiten betroffener Personen zu schützen. In der Praxis dürfte es jedoch wesentlich einfacher sein, die Verarbeitung auf die Gefahren eines personal data breach hin zu untersuchen als anhand eines noch näher zu bestimmenden Risikos für die Rechte und Freiheiten betroffener Personen. Wenn die Gefahren eines personal data breach adressiert werden können, sollte damit gleichzeitig auch mittelbar das Risiko für die Rechte und Freiheiten betroffener Personen adressiert werden können. Damit wird aus einer eher abstrakten und rechtlichen Bewertung eine klarere, technische Bewertung.

Ein weiteres praktisches Problem liegt darin, dass die Anforderungen an die Sicherheit für die gesamte Verarbeitung gelten und damit muss auch das angemessene Schutzniveau für die gesamte Verarbeitung gewährleistet werden.<sup>4</sup> In der Praxis dürfte es nicht hilfreich sein, ausschließlich ein Gesamtrisiko zu ermitteln. Verarbeitungen können mitunter sehr komplex sein und sich in viele verschiedenen Verarbeitungsprozesse aufteilen. Würde man versuchen bei solch komplexen Verarbeitungen einzig ein Gesamtrisiko zu ermitteln, könnten hier bereits schwerwiegende Fehler auftreten.<sup>5</sup> In der Regel dürfte es einzelne Verarbeitungsprozesse geben, die (deutlich) größere Risiken beinhalten als andere. Bei einem Gesamtrisiko könnten diese Besonderheiten nicht hinreichend erfasst werden. Das Problem dürfte sich anschließend auch fortziehen, wenn man versuchen würde, einzig anhand einer Gesamtbewertung das angemessene Schutzniveau und damit die zu treffenden TOM zu bestimmen. Es fehlt schlicht der Blick fürs Detail.

Daher wird hier vorgeschlagen, die Verarbeitung in die entsprechenden Verarbeitungsprozesse aufzuteilen.<sup>6</sup> Dies kann auch grafisch erfolgen. Anhand der

---

den „Sicherheitszielen“ und den „Gefährdungen“ abgeleitet. Siehe hingegen den Ansatz von *Bieker/Bremert*, ZD 2020, S. 7 ff., die eher die Rechte und Freiheiten als Ausgangspunkt nehmen, um (u.a. für Art. 32 DS-GVO) das Risiko zu bestimmen.

<sup>3</sup> Siehe hierzu: Kap. 4, C., III. *Anwendung auf (andere) Sicherheitsvorfälle*.

<sup>4</sup> Siehe hierzu: Kap. 5, A. *Risikobewertung*.

<sup>5</sup> Siehe ebenfalls im Rahmen der allgemeinen Risikobewertung die Gefahr, aufgrund der Komplexität der Verarbeitung, einzelne Risiken zu übersehen *Bieker/Bremert*, ZD 2020, S. 7, 11.

<sup>6</sup> Diesen Ansatz verfolgt wohl auch der Vorschlag von *Wennemann*, DuD 2018, S. 174, 176 f.; auch *Bieker/Bremert*, ZD 2020, S. 7, 11, sprechen sich in ihrem Vorschlag im Rahmen der allgemeinen Risikobewertung für eine Aufteilung komplexer Verarbeitung in einzelne Ab-

einzelnen Verarbeitungsprozesse können bestehende Besonderheiten leichter identifiziert werden, um sie bei der Risikobewertung gebührend zu berücksichtigen und anschließend auch zu adressieren. Die Sicherheit der Verarbeitung könnte man daher als die Summe der Sicherheit aller Verarbeitungsprozesse ansehen. Doch auch hier ist Vorsicht geboten. Falls sich bestimmte Gefahren erst aus der gesamten Verarbeitung ergeben, sollte man am Ende der Risikobewertung noch einmal eine Gesamtbetrachtung vornehmen, um diese Risiken zu identifizieren.<sup>7</sup>

Ein weiterer Vorteil dieser Methode besteht darin, dass Bewertungen einzelner Verarbeitungsprozesse auch für zukünftige Verarbeitungen verwendet werden können. Werden bspw. die Daten auf dem unternehmenseigenen Server gespeichert und es werden die Risiken für diesen bewertet, dann kann diese Bewertung auch Grundlage sein für alle anderen Verarbeitungen, bei denen Daten auf diesem Server gespeichert werden sollen. Natürlich muss die Bewertung anhand der verarbeitungsspezifischen Besonderheiten angepasst werden. Dennoch ließen sich die jeweiligen Verarbeitungsprozesse damit in Risikoklassen (bspw. von niedriges bis sehr hohes Risiko)<sup>8</sup> einteilen.

Diese Klassifizierung anhand von vergangenen Bewertungen kann dann für zukünftige Datenverarbeitungen, die ebenfalls diese Verarbeitungsprozesse enthalten, herangezogen werden. Dies kann zu Zeitersparnissen und reduziertem Aufwand bei der Erstellung der zukünftigen Risikobewertung führen. Allerdings sollte man darauf achten, dass die Risikobewertung anhand der individuellen Verarbeitungen erfolgt. Diese Individualitäten könnten in den eigenen Risikoklassen zwar bereits abgebildet sein. Dennoch muss in jedem Fall darauf geachtet werden, stets die Besonderheiten der jeweiligen Datenverarbeitung zu berücksichtigen. Basiert bspw. die Risikoklasse auf der Verarbeitung gewöhnli-

---

schnitte auf. Wohl gegen eine so kleinteilige Betrachtung v. *Lewinski/Rüpke/Eckhardt*, Datenschutzrecht, 2. Aufl. 2022, § 19, Rn. 15. Eine sehr ausdifferenzierte Aufteilung der Verarbeitung wird auch in DSK, Standard-Datenschutzmodell, Version 3.0, S. 36 ff., allgemein zur datenschutzrechtlichen Beurteilung, dargestellt.

<sup>7</sup> *Bieker/Bremert*, ZD 2020, S. 7, 11, sehen in ihrem Vorschlag daher eine abschließende Gesamtbetrachtung ebenfalls für geboten.

<sup>8</sup> Siehe zu Erstellung von Risikoklassen als Hilfsmittel sogleich und insb. die Nachweise in Fn. 10.

cher Daten und in der neuen Verarbeitung sollen nun besonders geschützte Daten verarbeitet werden, dürfte sich auch die Risikobewertung ändern und es könnten Anpassungen erforderlich sein.<sup>9</sup>

Weiterhin sorgt die Bildung solcher Risikoklassen und die Orientierung an diesen gleichzeitig dafür, dass aufgrund der Neubewertung einzelner Verarbeitungsprozesse mittelbar auch die alte Bewertung überprüft wird. So könnten Fehlbewertungen oder geänderte Umstände, die eine neue Bewertung der alten Verarbeitung rechtfertigen, schneller entdeckt werden.

Auch die eigentliche Bewertung des Risikos kann in der Praxis eine Herausforderung darstellen. In der Literatur wird als Hilfestellung für diese Bewertung die Bildung von Risikoklassen (bspw. niedriges, mittleres, hohes, sehr hohes Risiko) vorgeschlagen,<sup>10</sup> die aus einer Matrix aus Eintrittswahrscheinlichkeit und der Schwere der Folgen abgeleitet werden können.<sup>11</sup> Eine solche Darstellung kann durchaus hilfreich sein.

---

<sup>9</sup> Siehe hinsichtlich eines höheren Risikos bei besonders geschützten Daten: Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 50; vgl. auch Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27. Siehe ferner noch die Nachweise in Fn. 14, hinsichtlich der Berücksichtigung der Art der Daten im Rahmen der Angemessenheitsprüfung.

<sup>10</sup> Siehe allgemein zum Vorschlag zur Bildung von Risikoklassen im Rahmen des Art. 32 DS-GVO: Auer-Reinsdorff/Conrad/Conrad, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, § 33, Rn. 195, spricht von „Schutzbedarfskategorien“ und differenziert zwischen „Schutzklassen“ und „Risikoklassen“, wobei er anmerkt, dass die „Schutzbedarfsfeststellung“ und „Risikoanalyse“ nicht klar voneinander abgrenzbar seien (Rn. 188); Johannes/Geminn, InTeR 2021, S. 140, 142, sprechen hier von „Risikostufen“; Ehmann/Selmayr/Hladjk, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 DS-GVO, Rn. 11, spricht von „Schutzbedarfskategorien“; siehe auch Forgó/Helfrich/Schneider/Schmitz/v. Dall'Armi, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII, Kapitel 1, Rn. 54 mit Verweis auf Rn. 34 f. Siehe zur Klassifizierung allgemein im Zusammenhang der Risikobewertung: Ritter/Reibach/Lee, ZD 2019, S. 531, 533; Bieker/Bremert/Hansen, DuD 2018, S. 492, 494; DSK, Kurzpapier Nr. 18, S. 5; vgl. Knyrim/Pollirer, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.24, allgemein im Zusammenhang eines Informationssicherheits-Managementsystems; ähnlich Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 74 f.

<sup>11</sup> Siehe allgemein zur Darstellung im Rahmen einer Matrix aus Wahrscheinlichkeit und Schwere: Ritter/Reibach/Lee, ZD 2019, S. 531, 533, DSK, Kurzpapier Nr. 18, S. 5; vgl. wohl auch Bieker/Bremert/Hansen, DuD 2018, S. 492, 494; Knyrim/Pollirer, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.24; Moos/Schefzig/Arning/Heinemann, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 13, Rn. 74 f.; siehe auch Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 41, die im Zusammenhang des Art. 32 DS-GVO den Einsatz einer

Um diese Bewertung noch handhabbarer zu machen, sollte man genauso kleinschrittig vorgehen, wie bei der Identifizierung der Gefahren für einen personal data breach. Dabei sollte man sich dann aber nicht mehr nur auf die einzelnen Verarbeitungsprozesse konzentrieren. Das Risiko ist die Bewertung der Eintrittswahrscheinlichkeit und der Schwere der Folgen im Falle des Eintritts eines personal data breach. Daher sollte man innerhalb eines Verarbeitungsprozesses für die unterschiedlichen Gefahren eines personal data breach eine entsprechende Risikobewertung vornehmen. Im Zusammenhang dieser Bewertung sind dann aber auch die verarbeitungsspezifischen Umstände zu berücksichtigen. Streng genommen sind sie mit dem Verarbeitungskriterium Teil der Angemessenheitsprüfung.<sup>12</sup> Inhaltlich wirken sie sich jedoch auf das Risiko der Verarbeitung aus.<sup>13</sup>

So können sie sowohl den Bewertungsfaktor der Eintrittswahrscheinlichkeit beeinflussen. Wissen bspw. Angreifer, dass Finanzdaten<sup>14</sup> von einem Unternehmen massenweise erhoben werden, kann dies die Wahrscheinlichkeit von Angriffen erhöhen, da die Angreifer vermuten, wertvolle Daten zu „erbeuten“.<sup>15</sup>

---

Risikomatrix empfehlen. Siehe auch mit einer etwas anderen Darstellung Forgó/Helfrich/Schneider/Schmitz/v. Dall'Armi, *Betrieblicher Datenschutz*, 3. Aufl. 2019, Teil XII, Kapitel 1, Rn. 54 mit Verweis auf Rn. 34 f.

<sup>12</sup> Siehe hierzu: Kap. 7, B., III. *Verarbeitungskriterium*.

<sup>13</sup> Siehe hierzu: Kap. 7, B., III. *Verarbeitungskriterium*.

<sup>14</sup> Die Art der verarbeiteten Daten wird zwar nicht ausdrücklich im Verarbeitungskriterium benannt. Dass diese dennoch zu berücksichtigen ist, ergibt sich jedenfalls mittelbar aus den Kriterien, wie vor allem dem Zweck der Verarbeitung. Siehe allgemein zur Berücksichtigung der Art der Daten: Kühling/Buchner/Jandt, *DS-GVO – BDSG*, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 12; DatKomm/Pollirer, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 23 erfasst dies unmittelbar unter das Kriterium „Art“ (der Verarbeitung); so auch Kipker/Reusch/Ritter/Piltz/Zwerschke, *Recht der Informationssicherheit*, 2023, *Datenschutz-Grundverordnung*, Art. 32 DS-GVO, Rn. 26; siehe auch Simitis/Hornung/Spiecker gen. Döhmann/Hansen, *Datenschutzrecht*, 2019, Art. 32 DS-GVO, Rn. 27, die jedenfalls darauf verweist, dass aus der Sensibilität der Daten sich Risiken ergeben können; Freund u.a./Freund/Schöningh, *DSGVO*, 2023, Art. 32 DS-GVO, Rn. 50, sehen in der Verarbeitung sensibler Daten grds. höhere Risiken.

<sup>15</sup> Siehe LG Bonn, BeckRS 2020, 35663, Rn. 43 f., hinsichtlich einer größeren Wahrscheinlichkeit von Angriffen bei Interesse an wertvollen Daten, wobei dies im vorliegenden Fall abgelehnt wurde.

Gleichzeitig beeinflusst die Art der Daten auch den Faktor der Schwere der Folgen. Denn es macht einen Unterschied aus für die Folge, ob bspw. „gewöhnliche“ oder besondere Kategorien personenbezogener Daten von einem personal data breach betroffen sind.<sup>16</sup> Daher ist es sinnvoll, das Verarbeitungskriterium bereits auf dieser Ebene zu berücksichtigen.

Anzumerken ist an dieser Stelle, dass bei der Bewertung der Schwere der Folgen im Falle eines personal data breach, der hier vorgestellte, technische Ansatz an seine Grenzen stößt. Um die Folgen zu bewerten, geht es auch gerade um die Auswirkungen des personal data breach auf die Rechte und Freiheiten betroffener Personen. Eine technische Betrachtung ist hier nicht möglich. Dennoch sollte durch den Fokus auf die Gefahren des personal data breach auch diese rechtliche Betrachtung sichtbar erleichtert werden. Denn es bleibt ein Unterschied, ob man allgemein versucht, ein (abstraktes) Risiko für die Rechte und Freiheiten betroffener Personen zu ermitteln oder ob man dies anhand spezifischer Gefahren macht.

Nachdem die Bewertung der einzelnen Gefahren innerhalb der Verarbeitungsprozesse erfolgt ist, kann man versuchen, hieraus eine Gesamtschätzung für den gesamten Verarbeitungsprozess und schließlich für die gesamte Verarbeitung abzuleiten. Diese Betrachtung sollte allerdings dann vorrangig dazu dienen, um sich einen schnellen Überblick über die kritischen Verarbeitungen bzw. Verarbeitungsprozesse zu verschaffen, wenn es um einen groben Vergleich mit anderen Verarbeitungen oder Verarbeitungsprozessen geht.

## B. Bestandsaufnahme geeigneter TOM

Nachdem das Risiko der Verarbeitung bestimmt wurde, bedarf es vor der Reaktion auf dieses Risiko durch die Ermittlung des hierfür angemessenen Schutzniveaus einer Bestandsaufnahme geeigneter TOM. Ziel dieser Bestandsaufnahme ist es zunächst nur, sich einen Überblick zu verschaffen, welche Maßnahmen

---

<sup>16</sup> Vgl. allgemein den Einfluss der Daten, vor allem sensibler Daten, auf das Risiko: *DatKomm/Pollirer*, Stand: 76. EL. 2023, Art. 32 DS-GVO (Stand: Mai 2022), Rn. 23, der für diese Daten einen höheren Schutz nach Art. 32 DS-GVO fordert; *Simitis/Hornung/Spiecker gen. Döhmann/Hansen*, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 27; *Kühling/Buchner/Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 12.

überhaupt existieren, mit denen die identifizierten Risiken begegnet werden können.<sup>17</sup> Eine Bewertung der TOM erfolgt in diesem Schritt grds. noch nicht.

Indem allerdings alle denkbaren Maßnahmen aufgeführt werden, erfolgt aber unausweichlich eine erste Bewertung der tatsächlichen Verfügbarkeit und damit wohl auch des Abwägungskriteriums des Stands der Technik.<sup>18</sup> Damit zeigt sich aber schon, dass ein Schutzniveau, das aufgrund des Risikos über diese Maßnahmen hinausgehen würde, nicht gefordert werden könnte. Sollten sich daher bereits nach der Bestandsaufnahme Hinweise ergeben, dass die verfügbaren Maßnahmen das Risiko nicht ausreichend abdecken können, sollte darüber nachgedacht werden, die Datenverarbeitung auszusetzen und vorab eine tiefgreifendere Risikobewertung im Rahmen einer Datenschutz-Folgenabschätzung (vgl. Art. 35 DS-GVO) vorzunehmen<sup>19</sup> und dann ggf. eine vorherige Konsultation (vgl. Art. 36 DS-GVO) einer Aufsichtsbehörde in Erwägung zu ziehen.

In der Praxis dürfte eine umfassende Bestandsaufnahme aller in Frage kommenden Maßnahmen einen erheblichen Aufwand verursachen. Sofern keine Erfahrungswerte aus vergleichbaren Verarbeitungen bestehen, ließe sich der Aufwand auf mehreren Wegen reduzieren. Zum einen sollte man sich bei der Auflistung von Maßnahmen zunächst auf die einzelnen Verarbeitungsprozesse konzentrieren, wie bereits zuvor bei der Risikobewertung. Hiermit kann man sich auf einzelne Probleme konzentrieren und hierfür passende Maßnahmen identifizieren. Anschließend sollte der Verarbeiter auch hier noch einmal prüfen, ob mit den verfügbaren Maßnahmen auf der Einzelebene auch Risiken begegnet werden können, die sich ggf. erst aus dem Gesamtzusammenhang ergeben. Wenn nicht, muss der Verarbeiter hierfür noch einmal gesondert entsprechende Maßnahmen identifizieren.

---

<sup>17</sup> So auch Freund u.a./*Freund/Schöning*, DSGVO, 2023, Art. 32 DS-GVO, Rn. 42.

<sup>18</sup> Das Kriterium wird hier nicht abschließend definiert, siehe zu einer groben Einordnung allerdings: Kap. 7, B., I. *Stand der Technik*.

<sup>19</sup> Siehe allgemein dazu, dass die Risikobewertung im Rahmen des Art. 32 DS-GVO grds. nicht so ausführlich ausfallen muss, wie im Rahmen einer Datenschutz-Folgenabschätzung: Sy-dow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 8; Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 33.

Um die Bestandsaufnahme praktisch handhabbarer zu machen, ist es empfehlenswert, sich zunächst über allgemeine Sicherheitskonzepte (auf dem Abstraktionsgrad wie die Verschlüsselung oder die Pseudonymisierung)<sup>20</sup> Gedanken zu machen und diese anschließend durch einzelne Maßnahmen zu konkretisieren.<sup>21</sup>

Weiterhin sollte man berücksichtigen, dass ein wesentlicher Teil der finalen Angemessenheitsprüfung im Sinne des Datenverarbeiters erfolgt, um ihn vor unverhältnismäßigen Verpflichtungen zu schützen. Sofern sich kurzfristig Maßnahmen finden lassen, die das Risiko ausgleichen können und die für den Verarbeiter wirtschaftlich tragbar sind und keine rechtlichen Bedenken bestehen, sollte der Verarbeiter diese Maßnahmen auch ohne eine umfassende Angemessenheitsprüfung implementieren können. In diesen „eindeutigen Fällen“ kann die Prüfung dann auch kürzer ausfallen. Ob der Verarbeiter dann auf eine umfassende Prüfung zurückgreift, muss er im Rahmen seiner eigenen Kosten-Nutzen-Abwägung entscheiden. Ferner kann für den Verarbeiter auch ein Mittelweg geeignet sein. Sollte sich bei einzelnen Verarbeitungsprozessen herausstellen, dass diese hinsichtlich der Angemessenheitsprüfung problematisch werden, kann der Verarbeiter hier eine umfassende Prüfung vornehmen und sich bei weniger problematischen Prozessen schnell für passende Maßnahmen entscheiden, die die einzelnen Risiken ausgleichen.<sup>22</sup>

---

<sup>20</sup> Siehe zur Einordnung als Maßnahmenkategorien und nicht als konkrete Maßnahmen: Kap. 5, C., IV., 2., a) *Pseudonymisierung und Verschlüsselung (lit. a)*.

<sup>21</sup> Siehe in diese Richtung auch die Vorschläge im DSK, Standard-Datenschutzmodell, Version 3.0, S. 30 ff. zu „*generischen Maßnahmen*“, die für bestimmte Bereiche („*Bausteine*“, siehe <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>) wohl auch laufend ergänzt bzw. auch konkretisiert werden sollen (S. 67, 76 f.), wobei das Standard-Datenschutzmodell sich hier insgesamt mit der Umsetzung mittels technischer und organisatorischer Maßnahmen befasst und nicht nur auf Art. 32 DS-GVO begrenzt ist.

<sup>22</sup> Vgl. zu einem solchen Ansatz auch A-SIT/BKA, österreichisches Informationssicherheitshandbuch, Version 4.4.0, S. 157 ff., wonach es sich um einen „*kombinierten Ansatz*“ aus Grundschutz (mit Verweis (S. 136 ff.) auf den IT-Grundschutz des BSI, BSI-Standard 200-2, IT-Grundschutz-Methodik) und einer „*detaillierten Risikoanalyse*“ (S. 144 ff.) handele, bei der der Detailgrad der Risikoanalyse am zuvor festgestellten Schutzbedarf angepasst wird; siehe zu diesen drei Ansätzen ebenfalls Knyrim/*Pollirer*, Praxishandbuch Datenschutzrecht, 4. Aufl. 2020, Rn. 10.19. Siehe ebenfalls die Differenzierung hinsichtlich des Umfangs der Risikobewertung in Abhängigkeit von ihrer Kritikalität im Verhältnis zum Aufwand *Bieker/Bremert*, ZD 2020, S. 7, 12.



## C. Bewertung der TOM

Nachdem passende Maßnahmen identifiziert wurden, die das Risiko der Verarbeitung ausgleichen können, geht es im nächsten Schritt um die Bewertung dieser Maßnahmen. Die Maßnahmen sollten (mindestens)<sup>23</sup> hinsichtlich ihres tatsächlichen, wirtschaftlichen und rechtlichen „Aufwands“ bewertet werden. Hier geht es darum, den Abwägungskriterien Stand der Technik, Implementierungskosten und datenschutzrechtliche Bewertung eine entsprechende Gewichtung zu verschaffen. Um eine Vergleichbarkeit zwischen den einzelnen Maßnahmen zu erhalten, sollte eine Bewertungsskala verwendet werden. Ähnlich wie bei der Risikobewertung könnte man die Kriterien daher danach bewerten, ob die Implementierung mit einem „minimalen Aufwand“, einem „kleinen Aufwand“, einem „großen Aufwand“ oder einem „sehr großen Aufwand“ hinsichtlich des jeweiligen Kriteriums verbunden ist. Einen noch ausdifferenzierteren Vergleich könnte eine Punkteskala (bspw. von 0 = minimaler bzw. kein (nennenswerter) Aufwand bis 10 = sehr großer Aufwand) bieten.<sup>24</sup>

Die Bewertung der Maßnahmen hinsichtlich ihres Stands der Technik und ihrer Implementierungskosten stellt ein allgemeines Problem bei der Angemessenheitsprüfung nach Art. 32 Abs. 1 DS-GVO dar und bezieht sich nicht unmittelbar auf den Untersuchungsgegenstand. Daher wurden diese Abwägungskriterien in dieser Arbeit auch nicht abschließend definiert. Das bedeutet zwar nicht, dass nicht auch datenverarbeitende TOM anhand ihres Stands der Technik und ihrer Implementierungskosten bewertet werden müssen. Dennoch wird eine nähere Betrachtung dieser Bewertung hier nicht vorgenommen.

---

<sup>23</sup> Siehe hierzu: Kap. 7, C., II., 3. *Die datenschutzrechtliche Bewertung von TOM als unbekannter Abwägungstatbestand durch Auslegung der offenen Aufzählung.*

<sup>24</sup> Siehe allgemein kritisch zu dem Versuch einer ausdifferenzierten Risikobewertung: Moos/Schefzig/Arning/Schefzig, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 10, Rn. 19, wonach – im Rahmen eines allgemeinen Datenschutzmanagements – eine „*absolut genaue Risikoqualifizierung*“ zu einer „*Scheingenauigkeit*“ führen könnte; ähnlich *Bieker/Bremert/Hansen*, DuD 2018, S. 492, 494, die allgemein bei der Risikobewertung daher nur eine (grobe) Einteilung bspw. in „*leicht, mittel, schwer*“ vorschlagen, da es sonst zu einer Scheingenauigkeit käme; *Bieker/Bremert*, ZD 2020, S. 7, 8, die ein „*pseudo-mathematisch[es]*“ Vorgehen bei der Risikobewertung ablehnen; auch bereits kritisch im Rahmen der Risikoermittlung bei der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) *Bieker/Hansen/Friedewald*, RDV 2016, S. 188, 193. Wobei im Fokus der Kritik der Versuch einer detaillierten Risikoausweisung steht und es hier um die Bewertung der TOM geht. Allerdings dürfte die Kritik hierauf übertragbar sein.

Für den Untersuchungsgegenstand relevant ist hingegen die Bewertung des Abwägungskriteriums der datenschutzrechtlichen Bewertung datenverarbeitender TOM. Bei der Bewertung handelt es sich im Wesentlichen um die Prüfung einer Rechtsgrundlage für die Verarbeitung, wie sie im 3. Teil dargestellt wurde. Diese Prüfung kann allerdings nicht vollständig abgeschlossen werden. Denn an dieser Stelle lässt sich noch nicht abschließend klären, ob die Datenverarbeitung auch erforderlich ist, da es hier auf einen Ausgleich mit dem Zweck der Verarbeitung, also der konkreten Gewährleistung der Sicherheit der Verarbeitung ankommt.

Obwohl dieser Ausgleich mit dem Zweck erst später erfolgen kann und es damit an einer klaren Aussage darüber fehlt, ob die Datenverarbeitung nun rechtmäßig ist oder nicht, lassen sich bereits ohne diesen Ausgleich wichtige Erkenntnisse gewinnen. Wie bereits im 2. Teil dargestellt, kann das Abwägungskriterium der datenschutzrechtlichen Bewertung nicht nur zwischen erlaubten und verbotenen TOM differenzieren.<sup>25</sup> Grob gesagt lässt sich durch das Kriterium auch ausdrücken, wie kritisch die Rechtsordnung gegenüber den TOM steht.

Die „Einstellung“ der Rechtsordnung gegenüber datenverarbeitenden TOM lässt sich bereits aus der Datenverarbeitung als solche ableiten. Im Rahmen der Bewertung datenverarbeitender TOM geht es also zunächst darum, die Kritikalität der Datenverarbeitung zu bewerten. Tiefgreifende oder sehr umfassende Datenverarbeitungen sind mit einem höheren rechtlichen „Aufwand“ verbunden als bspw. vereinzelte und wenig umfangreiche Verarbeitungen.

#### D. Festlegung einer „Implementierungsreihenfolge“

Wurden alle Maßnahmen bewertet, geht es an die Vorbereitungen der Angemessenheitsprüfung. Hierfür sollten die Maßnahmen nach ihrem Aufwand sortiert werden, von Maßnahmen, die nur einen geringen Aufwand verursachen, bis hin zu Maßnahmen mit einem sehr großen Aufwand. Um dabei alle Aufwandskriterien gleichsam zu berücksichtigen, kann man aus den jeweiligen Einzelbewertungen einer Maßnahme eine Gesamtbewertung errechnen. Das Ziel

---

<sup>25</sup> Siehe hierzu: Kap. 7, C., III. *Konkretisierung des ungeschriebenen Abwägungskriteriums der datenschutzrechtlichen Bewertung von TOM.*

ist es, eine „Implementierungsreihenfolge“ zu bilden, mit deren Hilfe Datenverarbeiter für den Regelfall<sup>26</sup> die Sicherheit der Verarbeitung gewährleisten können, indem sie mit Maßnahmen beginnen, die für sie einen geringeren Aufwand verursachen und sich dann bei Bedarf aufwandsintensiveren Maßnahmen annähern.

Gleichzeitig findet in diesem Rahmen auch die Berücksichtigung des Tatbestands der Erforderlichkeit statt. Indem die Maßnahmen nach ihrem Aufwand sortiert werden, sollten Maßnahmen mit einer geringeren Datenverarbeitung am Beginn dieser Reihenfolge stehen und wären daher vorrangig zu implementieren. Damit lässt sich gewährleisten, dass zunächst versucht wird, die Sicherheit der Verarbeitung mit Maßnahmen zu erreichen, die keine oder nur eine geringe Datenverarbeitung brauchen. Erst wenn diese Maßnahmen nicht ausreichen, um ein angemessenes Schutzniveau sicherzustellen, werden dann anhand der Implementierungsreihenfolge Maßnahmen in Erwägung gezogen, die dateninvasiver sind.

Zu Wertungsproblemen kann hier allerdings die Zusammenrechnung der Aufwandskriterien führen. So können bspw. Maßnahmen mit einer dateninvasiven Datenverarbeitung und damit einem hohen rechtlichen Aufwand bei der Implementierungsreihenfolge weiter vorne stehen, wenn hingegen die beiden anderen Aufwandskriterien kaum vorhanden sind. Um diesem Problem zu begegnen, könnte man daran überlegen, ob man dem Kriterium der „datenschutzrechtlichen Bewertung“ eine größere Stellung einräumt, indem man bspw. mit Multiplikatoren arbeitet, die vorher auf die jeweiligen Kriterien angewandt werden. Eine solche Vorgehensweise könnte gerade von denen befürwortet werden, die scheinbar dem Kriterium der „Implementierungskosten“ einen geringeren Stellenwert zusprechen.<sup>27</sup>

Aus der Systematik des Art. 32 Abs. 1 DS-GVO lässt sich eine solche Ungleichbehandlung der Kriterien nicht ableiten. Allenfalls für die datenschutzrechtliche Bewertung datenverarbeitender TOM könnte ein solches Vorgehen gerechtfertigt werden. Dies ließe sich aber dann allenfalls aus dem Tatbestand der Erforderlichkeit begründen. Nach der hier vertretenen Ansicht ist eine stärkere Gewichtung nicht erforderlich, um eine angemessene Berücksichtigung der jeweiligen Wertungen zu gewährleisten. Der Tatbestand der Erforderlichkeit

---

<sup>26</sup> Siehe hinsichtlich einer Abweichung von dieser Implementierungsreihenfolge sogleich.

<sup>27</sup> Siehe hierzu: Kap. 7, C., I., 3. *Die teleologische Rechtfertigung für ein eigenes Abwägungskriterium.*

stellt auf einen Interessensausgleich ab, der sich bspw. in zumutbaren Alternativen, den Zweck der Verarbeitung zu erreichen, ausdrückt. Wenn andere Maßnahmen aufgrund ihres geringeren tatsächlichen und wirtschaftlichen Aufwands und einer invasiven Datenverarbeitung insgesamt zu einem geringeren Gesamtaufwand führen als Maßnahmen mit einer geringen Datenverarbeitung, dann sollte man dies grds. akzeptieren. Sollten im Einzelfall schwerwiegende Verschiebungen eintreten, kann man immer noch über eine Korrektur dieses Ansatzes, aber dann im Einzelfall, nachdenken. Ähnliche einzelfallbezogene Abweichungen von der Implementierungsreihenfolge wären denkbar, wenn sich bei Erstellung der Implementierungsreihenfolge aufwändigere Maßnahmen zeigen, die die Sicherheit deutlich wirkungsvoller gewährleisten. Auch hier ließe sich individuell überlegen, die ersten Maßnahmen der Implementierungsreihenfolge zu überspringen und gleich mit der Implementierung aufwändigerer aber dann wirkungsvollerer Maßnahmen zu beginnen.

Die (verständliche) Kritik an diesem Lösungsansatz darf an dieser Stelle aber nicht verschwiegen werden. Denn bei einer Lösung der hoch komplexen Abwägung beider Vorschriften auf Basis von mathematischen Vereinfachungen, werden nicht immer alle Entscheidungen perfekt sein.<sup>28</sup> Doch selbst auf diese Gefahr hin, ist diese Prüfung einer Alternative vorzuziehen, bei der nur abstrakt auf eine Interessenabwägung verwiesen wird. Denn eine abstrakte Interessenabwägung dürfte für die Praxis ein viel größeres Problem darstellen, zumal bei der starken Verflechtung der beiden Vorschriften eine solche Abwägung nicht ohne Einschnitte möglich wäre. Die Ergebnisse, die dabei am Ende herauskommen können, könnte die Interessenlage viel stärker missachten, als der hier dargestellte Prüfungsablauf im Regelfall erzeugt.

## E. Ableitung des angemessenen Schutzniveaus

Die entwickelte Implementierungsreihenfolge ist der Einstieg zur Bestimmung und Umsetzung des angemessenen Schutzniveaus. Für jede bestehende Gefahr

---

<sup>28</sup> Siehe bereits kritisch hinsichtlich einer detaillierten Risikobewertung bei der reinen Risikobewertung, die durch diesen Ansatz mit dem Problem der Berücksichtigung datenverarbeitender TOM noch erweitert wird, statt vieler: Moos/Schefzig/Arning/Schefzig, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 10, Rn. 19, im Rahmen eines allgemeinen Datenschutzmanagements; siehe für weitere Nachweise: Kap. 12, C. *Bewertung der TOM* und dort die Fn. 24.

eines personal data breach sollten nach der Reihe die Maßnahmen (beginnend bei den Maßnahmen mit dem geringsten Aufwand) daran bemessen werden, wie umfangreich sie die Gefahren eines personal data breach und somit das Risiko für die Rechte und Freiheiten betroffener Personen ausgleichen können. Sofern eine Maßnahme nicht ausreicht, die Gefahr eines personal data breach vollständig auszugleichen, ist anhand der Implementierungsreihenfolge die nächste, passende Maßnahme in Betracht zu ziehen. Wie oben bereits ausgeführt wurde,<sup>29</sup> wird eine vollständige Sicherheit wohl nicht gewährleistet werden können. Dennoch sollte sich an dieser Stelle das Vorgehen im Rahmen der Implementierungsreihenfolge an diesem Ideal ausrichten. Denn sofern dies nicht erreicht wird, stellt sich die Frage, welche weiteren Maßnahmen noch implementiert werden müssen.

An dieser Stelle wird dann die Berücksichtigung des Gebots der Verhältnismäßigkeit fortgesetzt. Denn ob eine (zusätzliche) Maßnahme zur (weiteren) Reduzierung des Risikos zu implementieren ist, sollte dann anhand einer „Kosten-Nutzen“-Entscheidung getroffen werden. Dabei geht es darum zu prüfen, ob einmal durch die Maßnahme eine Reduzierung des Risikos herbeigeführt wird, die im Verhältnis zum entstehenden Aufwand angemessen ist. Dieser Prozess wiederholt sich so lange, bis der weitere Aufwand für die Verbesserung der Sicherheit in keinem Verhältnis mehr zum Nutzen dieser Verbesserung steht.

Der Datenverarbeiter muss diese Schritte für alle Gefahren eines personal data breaches innerhalb jedes Verarbeitungsprozesses vornehmen. Sofern sich bei der Risikobewertung Gefahren eines personal data breach gezeigt haben, die sich erst aus mehreren Verarbeitungsprozessen oder der gesamten Verarbeitung ergeben, müssen diese dann noch gesondert adressiert werden. Wobei man hier allerdings prüfen könnte, ob diese übergreifenden Risiken nicht bereits durch Maßnahmen innerhalb einzelner Prozesse mit abgedeckt wurden. Aus der Summe ergibt sich dann das angemessene Schutzniveau für die gesamte Verarbeitung.

In diesem Vorschlag für die praktische Umsetzung zeigt sich dann auch etwas, das zuvor bei der rechtlichen Analyse kritisiert wurde. Denn die Bestimmung des angemessenen Schutzniveaus und die Auswahl hierfür geeigneter TOM sind so stark miteinander verknüpft, dass eine klare Trennung bei der

---

<sup>29</sup> Siehe hierzu: Kap. 5, B., I. *Bedeutung der Angemessenheit*.

praktischen Umsetzung nicht möglich ist.<sup>30</sup> Das ändert aber nichts daran, dass man diese Differenzierung bei der rechtlichen Analyse vornehmen muss.

## F. Überprüfung des angemessenen Schutzniveaus

Nachdem das angemessene Schutzniveau nach dem vorgeschlagenen Verfahren bestimmt und durch die entsprechenden Maßnahmen umgesetzt wurde, ist anschließend zu gewährleisten, dass die Sicherheit über die gesamte Verarbeitungsdauer aufrechterhalten wird.<sup>31</sup> Für den Datenverarbeiter bedeutet dies nicht nur, dass er während der Verarbeitung überprüfen muss, ob sich mit der Zeit etwas an seiner Risikobewertung geändert hat.<sup>32</sup> Zusätzlich bedarf es auch einer Überprüfung, ob die Maßnahmen weiterhin in der Lage sind, das Schutzniveau zu gewährleisten.<sup>33</sup> Ergibt die Überprüfung, dass die Anforderungen an die Sicherheit während der Verarbeitungsdauer nicht länger gewährleistet wird, müssen entsprechende Anpassungen vorgenommen werden.<sup>34</sup>

---

<sup>30</sup> Siehe hierzu: Kap. 5, B., III. Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?

<sup>31</sup> Siehe hierzu: Kap. 5, C., IV., 2., c) Überprüfungsverfahren (lit. d)).

<sup>32</sup> Vgl. Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 30; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 75 f.; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 20; vgl. auch Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 25, 58; Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 20, 54 f.

<sup>33</sup> Vgl. Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 58, 60; Simitis/Hornung/Spiecker gen. Döhmann/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 20, 54 f.; Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 78; siehe auch Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 20, der darauf verweist, dass Verfahren (hier konkret zur Pseudonymisierung und Verschlüsselung) ggf. durch bessere ersetzt werden müssen; ähnlich Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 75.

<sup>34</sup> Siehe auch Plath/Grages, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 8, der nicht nur die Wiederherstellung des Schutzniveaus erfasst, sondern auch eine „Absenkung“ (wohl aufgrund eines verringerten Risikos) anspricht; auch v.d. Bussche/Voigt/Voigt, Konzerndatenschutz, 2. Aufl. 2019, Teil 5, Kapitel 3, Rn. 14.

Wie eine solche Überprüfung und vor allem ein entsprechendes Überprüfungsmanagement im Detail aussehen kann, ist nicht Schwerpunkt dieser Arbeit. Wie jedoch bereits oben darauf hingewiesen wurde, ließen sich durch die kleinschrittige Untersuchung anhand einzelner Verarbeitungsprozesse Risikoklassen innerhalb des Unternehmens bilden, die als Anknüpfungspunkt für ein Überprüfungsmanagementsystem genutzt werden könnten.<sup>35</sup> Denn hierdurch lassen sich bereits bestehende Verarbeitungsprozesse im Rahmen einer neuen Verarbeitung erneut bewerten und können dann als Kontrolle älterer Verarbeitungen dienen.

Gleichzeitig können mit einer entsprechenden Dokumentation verdachtsbezogene Überprüfungen besser gesteuert werden. Auslöser solcher verdachtsbezogenen Überprüfungen könnten bspw. erkannte Angriffsversuche darstellen oder aber auch Gerichtsurteile, die sich mit einem vergleichbaren Verarbeitungsprozess auseinandergesetzt haben.<sup>36</sup> Durch die, für das hier dargestellte Verfahren, erforderliche Dokumentation können dann schneller die betroffenen Verarbeitungsprozesse identifiziert und neu bewertet werden.

Abschließend sollten aber auch verdachtslose Überprüfungen nach festgelegten Zeitabständen vorgenommen werden.<sup>37</sup> Dabei sollten die Zeitabstände

---

<sup>35</sup> Siehe hierzu: Kap. 12, A. *Identifikation und Bewertung des Risikos der Verarbeitung*.

<sup>36</sup> Siehe allgemein zur anlassbezogenen Überprüfung: Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 30; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 45; vgl. Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 21, mit dem Beispiel von bekanntgewordenen Sicherheitslücken; ähnlich Simitis/Hornung/Spiecker gen. Döhmman/Hansen, Datenschutzrecht, 2019, Art. 32 DS-GVO, Rn. 55; Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 80; siehe bspw. die Entscheidung des LG Bonn, BeckRS 2020, 35663, hinsichtlich einer Authentifizierungsmaßnahme im Rahmen des Art. 32 DS-GVO, aber auch konkret in Rn. 54, mit Verweis auf Gesetzesänderungen (in diesem Fall die Datenschutz-Grundverordnung selbst) als möglicher Anlass für eine Überprüfung.

<sup>37</sup> Siehe zur regelmäßigen Überprüfung: Kipker/Reusch/Ritter/Piltz/Zwerschke, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 60; Schuster/Grützmaker/Freund, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 60; Kühling/Buchner/Jandt, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 30; Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 44a f.; Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 77; Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, 21; Freund u.a./Freund/Schöning, DSGVO, 2023, Art. 32 DS-GVO, Rn. 78 f.; LG Bonn, BeckRS 2020, 35663, Rn. 54.

anhand des Risikos erfolgen.<sup>38</sup> Auch hier kann das kleinschrittige Verfahren des Lösungsvorschlags helfen, da es für die einzelnen Verarbeitungsprozesse das zugrundeliegende Risiko wesentlich detaillierter ausgibt als eine Risikobewertung der gesamten Verarbeitung.

---

<sup>38</sup> Kipker/Reusch/Ritter/*Piltz/Zwerschke*, Recht der Informationssicherheit, 2023, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 60; Schuster/Grützmaker/*Freund*, IT-Recht, 2020, 1. Teil EU-Recht, Datenschutz-Grundverordnung, Art. 32 DS-GVO, Rn. 60; Kühling/Buchner/*Jandt*, DS-GVO – BDSG, 4. Aufl. 2024, Art. 32 DS-GVO, Rn. 30; Paal/Pauly/*Martini*, DS-GVO BDSG, 3. Aufl. 2021, Art. 32 DS-GVO, Rn. 45; Schwartmann u.a./*Ritter*, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 77; Plath/*Grages*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 32 DS-GVO, Rn. 8; Sydow/Marsch/*Mantz*, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 21.



## Kapitel 13

### Darstellung anhand eines Beispiels

Das Spannungsverhältnis zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle im Rahmen datenverarbeitender TOM sollte innerhalb der Bestimmung des angemessenen Schutzniveaus i.S.d. Art. 32 Abs. 1 DS-GVO erfolgen. Die Prüfung teilt sich dabei in die wesentlichen Schritte (1) Risikobewertung, (2) Bestandsaufnahme geeigneter TOM, (3) Bewertung der TOM, (4) Festlegung einer Implementierungsreihenfolge, (5) Ableitung des angemessenen Schutzniveaus und (6) Überprüfung des angemessenen Schutzniveaus auf.

Nachfolgend soll die Prüfung anhand eines Beispiels dargestellt werden. Der hierbei zugrundeliegende (sehr vereinfachte) Sachverhalt gestaltet sich wie folgt:

*Ein Unternehmen möchte im Rahmen seines Kundenmanagements den Kunden ein Support- und Informationssystem zur Verfügung stellen. Kunden können hierüber Fragen bezüglich ihres Vertrages und den in diesem Zusammenhang anfallenden Daten klären. Dabei können Kunden einmal über die Internetseite des Unternehmens direkt auf ihre Daten zugreifen und diese selbst verwalten. Ergänzend sollen die Kunden aber auch die Möglichkeit erhalten, ihre Fragen an ein Support-Team zu stellen.<sup>1</sup>*

Unproblematisch werden im Rahmen dieses Support- und Informationssystems die personenbezogenen Daten der Kunden verarbeitet. I.S.d. Art. 32 DS-

---

<sup>1</sup> Siehe hinsichtlich der Authentifizierung der Kunden im Rahmen der Anforderungen des Art. 32 DS-GVO, worauf insbesondere sogleich noch eingegangen wird, auch die Entscheidung des LG Bonn, BeckRS 2020, 35663, das sich mit dieser Maßnahme im telefonischen Kundensupport auseinandersetzen musste; hierzu ebenfalls *Kiparski/Zirfas*, CR 2021, S. 108 ff.; siehe auch *Johannes/Geminn*, InTeR 2021, S. 140, 145 f. Wobei der Schwerpunkt wohl auf der Frage des Stands der Technik liegt und das Kriterium hier nicht abschließend definiert wurde.

GVO muss daher die Sicherheit für diese Verarbeitung gewährleistet werden. In einem ersten Schritt ist es erforderlich, das Risiko dieser Datenverarbeitung zu bestimmen, um anschließend das erforderliche Schutzniveau daraus abzuleiten. Um dies praktisch handhabbarer zu machen, wird hier vorgeschlagen, sich an den einzelnen Verarbeitungsprozessen zu orientieren. Dazu bietet es sich hier zunächst an, die Verarbeitung grafisch darzustellen.

Dies könnte hier – zum Zwecke der Übersicht vereinfacht – wie folgt aussehen:

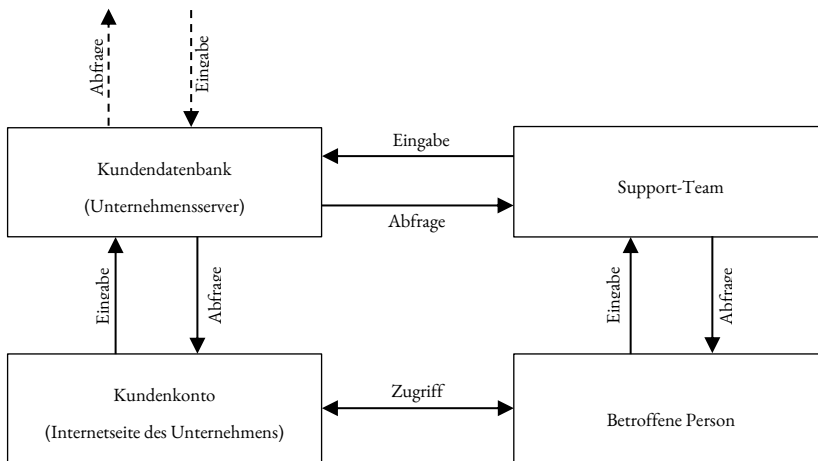


Abb. 8: Vereinfachte Darstellung einer Verarbeitung im Rahmen eines CRM-Prozesses (eigene Darstellung)

Die Beschreibung der Verarbeitung muss anschließend durch die bestehenden Gefahren eines personal data breaches ergänzt werden. Auch hier sind die Gefahren den einzelnen Verarbeitungsprozessen zuzuordnen. Betrachtet man sich hier konkret das Verhältnis zwischen den anfragenden, betroffenen Personen und dem Support-Team, dann lässt sich hier bspw. die Gefahr einer unberechtigten Abfrage von personenbezogenen Daten durch unbefugte Personen nennen (unbefugte Offenlegung bzw. unbefugter Zugang). Weiterhin könnte aber auch die Gefahr einer unbeabsichtigten Vernichtung oder Veränderung

von Daten bestehen, wenn im Rahmen der Anfrage die Daten gelöscht oder geändert werden. Dies kann durch mögliche Falschangaben der betroffenen Person selbst geschehen oder durch einen Übertragungsfehler des Support-Teams.

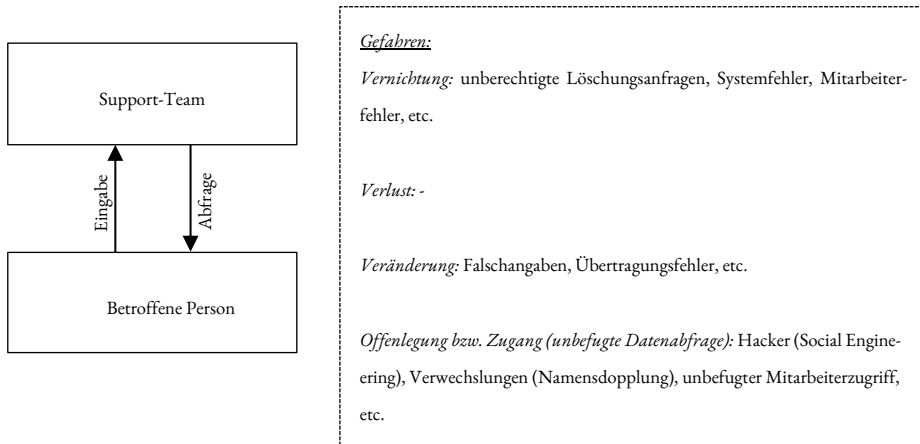


Abb. 9: Zuordnung der Gefahren anhand eines Ausschnitts aus Abb. 8 (eigene Darstellung)

Wurden für sämtliche Prozesse innerhalb der Verarbeitung die Gefahren eines personal data breaches ermittelt, kann nun die Risikobewertung erfolgen. Dabei geht es darum, die Eintrittswahrscheinlichkeiten eines personal data breach und die daraus resultierende Schwere für die Rechte und Freiheiten betroffener Personen zu bewerten. Hierzu könnte das Risiko in einem Punktesystem dargestellt werden. Das Risiko ist dabei abhängig von der jeweiligen Verarbeitung und den Umständen. Im Rahmen dieses vereinfachten und gekürzten Beispiels kann eine genaue Risikobewertung nicht vorgenommen werden. Um das Prüfungsschema zu veranschaulichen, ist dies aber auch nicht erforderlich. Im Falle einer unberechtigten Datenabfrage wird hier als Prämisse von einem mittleren Risiko ausgegangen. Auf einer Punkteskala von 0 (kein bzw. ein vernachlässigbares Risiko) bis 10 (nicht akzeptables Risiko) könnte man einen Wert von 4 bis 6 Punkten annehmen.<sup>2</sup>

<sup>2</sup> Siehe kritisch hinsichtlich einer detaillierten Risikobewertung, statt vieler: Moos/Schefzig/Arning/Schefzig, Praxishandbuch DSGVO, 2. Aufl. 2021, Kap. 10, Rn. 19, im Rahmen eines allgemeinen Datenschutzmanagements; siehe für weitere Nachweise: Kap. 12, C. *Bewertung der TOM* und dort die Fn. 24.

Wurden alle Einzelrisiken der Verarbeitung bestimmt, geht es als nächstes darum, den hierfür erforderlichen Schutz zu bestimmen. Da Art. 32 Abs. 1 DS-GVO ein angemessenes Schutzniveau fordert und damit Aufwand und Risiko ins Verhältnis zueinander setzt, bedarf es zunächst einer Bestandsaufnahme möglicher Maßnahmen. Auch hier sollte man denkbare Maßnahmen auf die einzelnen Gefahren ausrichten.

Um bspw. die Gefahr einer unbefugten Datenabfrage zu begegnen, kommt ein Authentifizierungssystem in Betracht, mit dem sich die anfragende Person als berechtigt ausweisen muss. Konkret könnte dies in Gestalt der Abfrage des Geburtsdatums erfolgen. Auch die Angabe eines vorab definierten Kundenkennworts könnte als Authentifizierung dienen. Ferner könnte auch eine Zwei-Faktor-Authentifizierung erfolgen, bei der neben einem persönlichen Kennwort die Kunden bspw. ihr Konto mit einer Smartphone-App verbinden und die Mitarbeiter des Support-Teams hierüber eine TAN an das Smartphone des Kunden senden, die der Kunde angeben muss.

Um die Gefahren einer unbefugten Datenabfrage zu reduzieren, könnte ferner überlegt werden, die Daten, die über das Support-Team herausgegeben werden dürfen, zu begrenzen. So könnte man bspw. für besonders sensible Daten andere Verfahren etablieren, um diesbezügliche Kundenabfragen zu bearbeiten. Dies führt zwar dazu, dass dadurch eine weitere Datenverarbeitung entsteht, die dann auch wieder nach den Anforderungen des Art. 32 DS-GVO zu schützen ist. Für die hier betrachtete Datenverarbeitung ließe sich damit aber das Risiko reduzieren und könnte so differenzierter auf die Risiken der Verarbeitung reagieren.

Während es sich bei den verschiedenen Authentifizierungssystemen um unterschiedliche Ausgestaltungen derselben Maßnahmenkategorie handelt, die in Konkurrenz zueinander treten, lassen sich ein Authentifizierungssystem und Einschränkungen möglicher Datenabfragen über das Support-Team miteinander kombinieren.

Gefahren	Maßnahmen(-kategorien)
Unbefugte Datenabfrage	1. Authentifizierungssystem - Abfrage des Geburtsdatums - Abfrage eines Kundenkennworts - Zwei-Faktor-Authentifizierung (Smartphone-App)
	2. Einschränkung der Datenabfrage - Anweisung an Mitarbeiter über (eingeschränkte) Datenherausgabe - Einschränkung der Zugriffsrechte der Mitarbeiter
	3. [...]
Unbefugte Veränderung des Datenbestands	1. Bestätigung durch Kunden
	2. 4-Augen-Prinzip
	3. Plausibilitätskontrolle
	4. [...]

Abb. 10: Gegenüberstellung von Gefahren und Maßnahmen(-kategorien) (eigene Darstellung)

Nachdem für sämtliche Gefahren die denkbaren Maßnahmen herausgearbeitet wurden, müssen diese bewertet werden. Dies erfolgt mindestens anhand der Kriterien des Stands der Technik, der Implementierungskosten und der datenschutzrechtlichen Bewertung. Wie oben vorgeschlagen,<sup>3</sup> könnte jedes Kriterium von 0 (kein bzw. sehr geringer Aufwand) bis 10 (sehr hoher Aufwand) bewertet werden.

Die Kriterien Stand der Technik und Implementierungskosten wurden im Rahmen dieser Arbeit nicht abschließend definiert. Dies gilt vor allem für das

<sup>3</sup> Siehe hierzu: Kap. 12, C. Bewertung der TOM.

Kriterium Stand der Technik. Eine solche Definition soll auch hier nicht erfolgen und ist für die Darstellung des Prüfungsablaufs auch nicht unbedingt notwendig. Nach dem hier zugrunde gelegten Verständnis ist von dem Kriterium „Stand der Technik“ nur der tatsächliche Aufwand für die Implementierung der Maßnahmen erfasst. Aufgrund der fehlenden, abschließenden Herleitung einer Definition, werden für die „Bewertung“ der beiden Kriterien „Stand der Technik“ und „Implementierungskosten“ nachfolgend Fantasiezahlen verwendet.

Geht es um die datenschutzrechtliche Bewertung der Maßnahmen, so werden im Rahmen der Authentifizierungssysteme personenbezogene Daten (Geburtsdatum, persönliches Kundenkennwort und die Daten, die durch die Verknüpfung mit einer Smartphone-App anfallen) verarbeitet. Es handelt sich insofern um datenverarbeitende TOM. Die datenschutzrechtlichen Eingriffe dieser Verarbeitung dürften aber unterschiedlich stark ausfallen.

Die Abfrage des Geburtsdatums dürfte von niedriger bis mittlerer Eingriffsschwere sein. Es handelt sich hier um eine zusätzliche Information über die betroffene Person, die allerdings nicht als wirkliches Geheimwissen eingeordnet werden kann.<sup>4</sup> Die datenschutzrechtliche Bewertung könnte sogar niedriger ausfallen, wenn bereits in dem ursprünglichen Datensatz das Geburtsdatum enthalten ist und es sich somit um keine „zusätzliche“ Information handelt.

Dagegen sollte ein Kundenkennwort keine eigenen, persönlichen Elemente über die betroffene Person aufweisen. Ihre Einordnung als personenbezogenes Datum rührt vielmehr nur daher, dass hiermit eine Zuordnung zur betroffenen Person hergestellt werden kann, weil es ihr „persönliches“ Kennwort ist. Diese Einschätzung erfolgt unter der Annahme, dass Personen bei der Vergabe eines Kennworts beachten, gerade keine persönlichen Elemente, wie Geburtstage, die Namen oder Initialen von Familienangehörigen zu verwenden. Doch selbst wenn sich Personen dafür entscheiden sollten, solche persönlichen Angaben in ihren Kennwörtern zu machen, dürfte es den Datenverarbeitern bei der Sicherheitsbewertung nicht zuzurechnen sein. Zumindest dann nicht, wenn diese noch einmal auf die wesentlichen Elemente eines sicheren Passworts hinweisen. Daher ist die datenschutzrechtliche Bewertung hier als niedrig anzusehen.

---

<sup>4</sup> Siehe hierzu auch die Einschätzung des LG Bonn, BeckRS 2020, 35663, Rn. 49 f., jedoch dann hinsichtlich der Frage, ob hiermit ein wirksamer Schutz durch die Authentifizierung besteht.

Die Bewertung der Zwei-Faktor-Authentifizierung (bspw. die Kombination aus einem persönlichen Kennwort und einer TAN) dürfte hingegen zu einer höheren datenschutzrechtlichen Bewertung führen. Dies liegt aber weniger an den Informationen, also Kennwort und TAN, selbst, da diese – wie gerade beim isolierten Kundenkennwort bereits angesprochen – keine persönlichen Informationen enthalten (sollten). Die datenschutzrechtlichen Bedenken dürften eher mit dem „Übertragungsweg“ der Authentifizierung des zweiten Faktors zusammenhängen. Abschließend lässt sich dies hier zwar anhand dieses einfachen Beispiels nicht sagen, da es darauf ankommen wird, welche Informationen durch die Verknüpfung des Kontos mit dem zweiten Faktor (hier Smartphone-App) alles verarbeitet werden. Wahrscheinlich ist, dass hier aber zumindest Informationen wie die Telefonnummer und Angaben zum Gerät enthalten sind.

Die Beschränkung der Daten, die von den betroffenen Personen über das Support-Team abgefragt werden können, dürfte selbst hingegen zu keiner Verarbeitung personenbezogener Daten führen.

Um noch kurz auf die beiden anderen Faktoren, Stand der Technik und Implementierungskosten, einzugehen, dürfte der tatsächliche (Stand der Technik) und wirtschaftliche (Implementierungskosten) Aufwand bei der Abfrage des Geburtsdatums nicht sehr hoch sein, vor allem wenn dieses sich bereits in dem Datensatz befindet.<sup>5</sup> Hier dürften entsprechende Handlungsanweisungen an die Mitarbeiter des Support-Teams und Schulungen genügen.<sup>6</sup> Ähnliches dürfte für die Einschränkung der Datenherausgabe gelten.

Etwas aufwändiger könnte da schon die Vergabe eines Kundenkennworts sein, dass vorab festgelegt werden muss und hierfür ggf. entsprechende Anpassungen zur Hinterlegung gemacht werden müssten.<sup>7</sup> Der Einsatz einer Zwei-

---

<sup>5</sup> Das LG Bonn, BeckRS 2020, 35663, Rn. 48 ff. hat in diesem konkreten Fall die Abfrage von Namen und Geburtsdatum als Authentifizierung für unzureichend erklärt. Siehe jedoch auch Rn. 51, wo das Gericht (zwar im Zusammenhang mit „Spezialwissen“) gerade darauf hinweist, dass die Kosten gering sein dürften, wenn die abgefragten Daten bereits im Datensatz vorhanden sind.

<sup>6</sup> Siehe LG Bonn, BeckRS 2020, 35663, Rn. 51, zwar in Bezug auf „Spezialwissen“ wie „Kunden- oder Rechnungsnummer“, welches aber ebenfalls im Datensatz enthalten ist.

<sup>7</sup> Siehe Kiparski/Zirfas, CR 2021, S. 108, Rn. 16, mit der Einschätzung, dass bei der „Abfrage echten Geheimwissens“ im Vergleich zu „allgemeinerem Wissen“ (wie dem Geburtsdatum) wohl keine großen Steigerungen der Implementierungskosten zu erwarten sind. Unklar ist jedoch, ob unter „Geheimwissen“ hiernach auch ein eigenes Benutzerkennwort fällt oder ob hier nicht auf Daten wie Kunden- oder Rechnungsnummern verwiesen wird (siehe LG Bonn,

Faktor-Authentifizierung hingegen dürfte einen höheren tatsächlichen und wirtschaftlichen Aufwand verursachen, da hierzu gerade ein entsprechendes „Übermittlungsverfahren“ für den zweiten Faktor geschaffen werden muss, bspw. die Entwicklung oder der Einkauf einer Smartphone-App.<sup>8</sup> Auch die Beschränkung der Zugriffsrechte der Mitarbeiter geht über einfache Handlungsanweisungen hinaus und dürfte eine aufwändigere, technische Umsetzung erfordern.

Die Bewertung der Maßnahmen könnte für die Gefahr einer unbefugten Datenabfrage daher wie folgt aussehen:

Maßnahme	Stand der Technik	Implementierungskosten	Datenschutzrechtliche Bewertung	Gesamtbewertung
Abfrage des Geburtsdatums	2	2	3	2,3
Abfrage eines Kundenkennworts	3	2	1	2
Zwei-Faktor-Authentifizierung	6	7	6	6,3
Einschränkung der Datenherausgabe (Anweisung an Mitarbeiter)	3	2	1	2
Einschränkung der Zugriffsrechte der Mitarbeiter	4	5	1	3,3

Abb. 11: Bewertung der technischen und organisatorischen Maßnahmen (eigene Darstellung)

Anschließend sollte anhand des Gesamtaufwands eine Implementierungsreihenfolge generiert werden:

BeckRS 2020, 35663, Rn. 51). Siehe sonst auch die Einschätzungen hinsichtlich der Implementierung einer PIN in der nachfolgenden Fußnote.

<sup>8</sup> Siehe hierzu die Ausführungen zur Implementierung einer PIN und den damit verbundenen Prozessen und Kosten LG Bonn, BeckRS 2020, 35663, Rn. 17; siehe auch *Kiparski/Zirfas*, CR 2021, S. 108, Rn. 16 mit Hinweis auf die damit verbundenen, „technische[n] Umstellungen“ und „bobe[n] Implementierungskosten“.



Maßnahme	Gesamtbewertung	Rang
Abfrage des Geburtsdatums	2,3	2
Abfrage eines Kundenkennworts	2	1
Zwei-Faktor-Authentifizierung	6,3	4
Einschränkung der Datenherausgabe (Anweisung an Mitarbeiter)	2	1
Einschränkung der Zugriffsrechte der Mitarbeiter	3,3	3

Abb. 12: Reihenfolge für die Implementierung technischer und organisatorischer Maßnahmen (eigene Darstellung)

Ausgehend von dieser Implementierungsreihenfolge sollte das angemessene Schutzniveau abgeleitet werden. Das bedeutet, dass zu prüfen ist, mit welchen Maßnahmen das Risiko angemessen begegnet wird. Hier ist darauf zu verweisen, dass die Bewertungen über das Risiko auf der einen Seite und die Bewertungen auf Seiten des Aufwands nicht miteinander zu verrechnen sind. Vielmehr kommt es darauf an zu beurteilen, ob das (Rest-)Risiko im Verhältnis zum (weiteren) Aufwand hinnehmbar ist.

So dürfte das Risiko im Falle einer unberechtigten Datenabfrage bereits durch die Implementierung eines Authentifizierungsverfahrens ausreichend abgesenkt sein. Sollte das Restrisiko hier, ggf. aufgrund der Verarbeitung besonders sensibler Daten, sehr hoch sein, sollte man weitere Maßnahmen implementieren, bspw. indem man den Umfang der Datenabfrage über das Support-Team begrenzt. Dieser Abgleich zwischen den Maßnahmen und dem Risiko muss für sämtliche Einzelrisiken erfolgen, um das angemessene Schutzniveau für die gesamte Verarbeitung zu bestimmen und anschließend umzusetzen.

An dem Beispiel zeigt sich eine Besonderheit, auf die bei der allgemeinen Darstellung des Prüfungsablaufs noch nicht eingegangen werden konnte. Lassen sich mehrere Maßnahmen unter einer Maßnahmenkategorie fassen, wie dies hier für die verschiedenen Formen der Authentifizierungsverfahren der Fall ist, kann es sein, dass Maßnahmen innerhalb der Implementierungsreihenfolge übersprungen werden müssen. Denn wird bereits ein Authentifizierungsverfahren mittels Passwortabfrage schon implementiert und das Risiko wäre hier noch nicht ausreichend reduziert, so wäre es im Rahmen der Implementierungsreihenfolge nicht zielführend, über die Implementierung eines (weiteren) Authentifizierungsverfahren mittels Angabe des Geburtsdatums nachzudenken. Zwar

könnte man überlegen, weitere oder „schwierigere“ Informationen zwecks Authentifizierung abzufragen, um das Risiko einer unbefugten Datenabfrage durch Identitätsdiebstahl zu verhindern. Dafür bedarf es aber kein zusätzliches Verfahren. Daher würde es für die Absenkung des Risikos keinen Mehrwert haben, ein solches zu implementieren.

In diesem Fall, in dem das Risiko weiterhin zu hoch ist, sollte man daher nicht stoppen und die nachfolgenden Maßnahmen der Implementierungsreihenfolge außer Acht lassen. Denn spätere Maßnahmen könnten aufgrund anderer Wirkungsweisen das Risiko weiter reduzieren. Können daher andere Maßnahmen aus derselben Maßnahmenkategorie das Risiko nicht weiter reduzieren, sollten diese in der Implementierungsreihenfolge übersprungen werden und die Prüfung des angemessenen Schutzniveaus anhand der nächsten Maßnahmen (vorrangig wohl) aus einer anderen Maßnahmenkategorie fortsetzen.

Nachdem das Schutzniveau bestimmt und auch umgesetzt wurde, muss die Sicherheit der Verarbeitung abschließend überwacht werden. Dies sollte einmal, ausgehend von dem jeweiligen Risiko, regelmäßig erfolgen. Da es sich zumindest bei dem Risiko der unberechtigten Datenabfrage hier eher um ein mittleres Risiko handeln dürfte, darf der Abstand zwischen den Überprüfungen etwas länger (ca. zwei Jahre) betragen.<sup>9</sup>

Daneben sollten aber auch anlassbezogene Überprüfungen erfolgen. Einen solchen Anlass könnten hier bspw. eingetretene Sicherheitsvorfälle sein. Wird dem Unternehmen bekannt, dass es bspw. zu unberechtigten Datenabfragen gekommen ist, dann müssen sowohl das Risiko als auch die eingesetzten Maßnahmen überprüft werden. Ebenfalls Anlass zu einer Überprüfung könnten bspw. Entscheidungen der Aufsichtsbehörden oder Gerichte in ähnlichen Fällen sein.

---

<sup>9</sup> Siehe Schwartmann u.a./Ritter, DS-GVO/BDSG, 2. Aufl. 2020, Art. 32 DS-GVO, Rn. 77, der wohl zwei Jahre für das Maximum zwischen den Überprüfungen ansieht, stellt aber insgesamt auf das Risiko ab; siehe auch Sydow/Marsch/Mantz, DS-GVO – BDSG, 3. Aufl. 2022, Art. 32 DS-GVO, Rn. 21, wobei nicht klar ist, ob die zwei Jahre nur als Beispiel gemeint sind oder die Obergrenze sein soll, zumal er ebenfalls auf das Risiko abstellt.

Als der BfDI das Bußgeld gegen 1&1 aufgrund einer unzureichenden Authentifizierung verhängt hat,<sup>10</sup> sollte dies bei (anderen) Unternehmen zum Anlass genommen werden, die eigenen Verarbeitungen dahingehend neu zu bewerten.<sup>11</sup> Aber auch das darauffolgende Urteil des Landgericht Bonn<sup>12</sup> sollte anschließend in die Bewertung mit aufgenommen werden.

---

<sup>10</sup> BfDI, Pressemitteilung 30/19, 09.12.2019.

<sup>11</sup> Siehe allerdings *Kiparski/Zirfas*, CR 2021, S. 108, Rn. 49, mit der kritischen Anmerkung in Bezug auf den Tatbestand „Stand der Technik“, dass die Auffassungen der Aufsichtsbehörden nicht (faktisch) dazu führen dürften, den Stand der Technik festzulegen, da dieser sich aus den „Anforderungen des Art. 32 Abs. 1 [D]SGVO“ ergibt.

<sup>12</sup> LG Bonn, BeckRS 2020, 35663.



## Kapitel 14

# Übertragbarkeit der Lösung

Die Arbeit behandelt das Spannungsverhältnis zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle bei datenverarbeitenden TOM und formuliert einen Lösungsvorschlag, wie diese beiden Bereiche des Datenschutzrechts miteinander in Einklang gebracht werden können. Im Fokus stehen dabei die datenverarbeitenden TOM und die rechtlichen Anforderungen, die Art. 6 DS-GVO an die ihnen zugrundeliegende Datenverarbeitung stellt. Auch wenn der Gegenstand der Arbeit sich hierauf beschränkt und der Lösungsvorschlag auf die spezifischen Aspekte der beiden, in Konflikt stehenden Regelungen des Art. 32 DS-GVO und Art. 6 DS-GVO zugeschnitten ist, können aus den Erkenntnissen dieser Arbeiten Ableitungen getroffen werden, die sich auch auf andere, aber ähnliche Bereiche anwenden lassen.

### A. Datenverarbeitende TOM als Teil einer Gruppe vergleichbarer Maßnahmen

Dabei muss man sich zunächst bewusst machen, dass datenverarbeitenden TOM stellvertretend für eine deutlich größere Gruppe von technischen und organisatorischen Maßnahmen stehen. Verallgemeinert gesagt, handelt es sich bei datenverarbeitenden TOM um Maßnahmen, an deren Implementierung die Rechtsordnung zusätzliche Anforderungen stellt. Bei datenverarbeitenden TOM sind dies eben die Anforderungen an die rechtmäßige Verarbeitung personenbezogener Daten, die mit der Implementierung und Durchführung der Maßnahmen einhergeht. Zusätzliche Anforderungen an die Implementierung von technischen und organisatorischen Maßnahmen beschränken sich allerdings nicht zwingend auf das Datenschutzrecht. Auch andere Rechtsgebiete

könnten an die Implementierung von Maßnahmen, die der Erfüllung der Sicherheit der Verarbeitung dienen, zusätzliche Anforderungen stellen.

Beschränkt man sich nicht einzig auf datenverarbeitende TOM könnte man daher diese Gruppe auf alle technischen und organisatorischen Maßnahmen erweitern, an deren Implementierung die Rechtsordnung zusätzliche Anforderungen knüpft. In all diesen Fällen entsteht ein ähnliches Spannungsverhältnis zwischen Art. 32 DS-GVO und dem jeweiligen Rechtsgebiet, dass die Anforderungen an die Implementierung der TOM stellt. Nachfolgend soll daher dargestellt werden, wie die hier gewonnenen Erkenntnisse und Lösungen auch in den Bereichen Anwendung finden können, in denen die Sicherheit der Verarbeitung in Konflikt mit anderen Rechtsvorschriften steht.

## B. Von der „datenschutzrechtlichen Bewertung“ hin zur „rechtlichen Bewertung“

Das wesentliche Instrument für die Lösung des Spannungsverhältnisses liegt im Rahmen der Sicherheit der Verarbeitung in dem Abwägungskriterium der datenschutzrechtlichen Bewertung technischer und organisatorischer Maßnahmen. Bisher wurde dieses Kriterium vorrangig im Kontext der Anforderung an TOM durch die datenschutzrechtliche Vorabkontrolle i.S.d. Art. 6 DS-GVO behandelt.

Die Rechtfertigung für ein solches Abwägungskriterium im Rahmen der Angemessenheit des Schutzniveaus nach Art. 32 DS-GVO zeigte aber bereits, dass sich dieses Kriterium nicht auf die datenschutzrechtliche Bewertung von TOM beschränken muss. Das Telos dieses Kriteriums liegt vielmehr allgemein darin, dass neben tatsächlichen und wirtschaftlichen Aspekten auch die rechtliche Ebene in die Angemessenheitsprüfung mit aufzunehmen ist. Allgemein können rechtliche – und eben nicht nur datenschutzrechtliche – Anforderungen an die Implementierung von TOM für Datenverarbeiter zu vergleichbaren Hindernissen bei der Umsetzung der Sicherheit führen, wie tatsächliche und vor allem wirtschaftliche Hindernisse.<sup>1</sup>

Damit lässt sich das Abwägungskriterium auch für Spannungsverhältnisse zwischen der Sicherheit der Verarbeitung und den rechtlichen Anforderungen

---

<sup>1</sup> Siehe hierzu: Kap. 7, C., I., 3. *Die teleologische Rechtfertigung für ein eigenes Abwägungskriterium* und 4. *Zwischenergebnis*.

an die Implementierung von TOM aus anderen Teilen der Rechtsordnung rechtfertigen. Anstelle eines Kriteriums der „datenschutzrechtlichen Bewertung“ kann man daher allgemein von der „rechtlichen Bewertung von TOM“ sprechen.

### C. Gesonderte Beachtung der „Regulierungsvorschriften“

Der 3. Teil dieser Arbeit befasst sich mit den Anforderungen an die rechtmäßige Verarbeitung personenbezogener Daten im Rahmen der datenschutzrechtlichen Vorabkontrolle nach Art. 6 DS-GVO. Im Lichte des Art. 32 DS-GVO geht es hierbei um die (datenschutz-)rechtliche Bewertung der datenverarbeitenden TOM. Für die Übertragung auf andere Rechtsgebiete hat dieser Teil somit keine Bedeutung. Aufgrund des Fokus dieser Arbeit auf datenverarbeitende TOM sind in hiesigem Ansatz die speziellen Regulierungsvorschriften aus anderen Rechtsgebieten daher nicht berücksichtigt und sollen auch jetzt nicht mehr im Detail dargestellt werden. Die nachfolgenden Ausführungen beschränken sich daher auf die wesentlichen Grundzüge für die Übertragbarkeit der Erkenntnisse auf andere Rechtsgebiete.

Anstelle der datenschutzrechtlichen Bewertung müssen die jeweils einschlägigen, rechtlichen Anforderungen an die TOM aus den in Frage stehenden Rechtsgebieten untersucht werden. Dabei muss man differenzieren, ob diese Anforderungen statisch oder – wie im Fall des Datenschutzrechts – dynamisch ausgestaltet sind. Damit ist gemeint, dass es Rechtsvorschriften geben kann, die bestimmte Maßnahmen schlicht verbieten. Die datenschutzrechtliche Vorabkontrolle, als Beispiel für eine dynamische Vorschrift, verbietet datenverarbeitende TOM (bzw. die zugrundeliegende Datenverarbeitung) hingegen nicht pauschal. Ob eine Datenverarbeitung rechtmäßig ist, ist von den jeweiligen Umständen abhängig. Im Falle der datenschutzrechtlichen Vorabkontrolle ist vor allem das Verhältnis der Datenverarbeitung zum Verarbeitungszweck und die Bewertung, ob die Datenverarbeitung hierfür erforderlich ist von Bedeutung. Auch andere Vorschriften können ein ähnliches System verfolgen. So steht zwar die Rechtsordnung der Implementierung dieser TOM kritisch gegenüber. Eine finale Entscheidung über ihre Zulässigkeit wird aber von weiteren Faktoren abhängig gemacht.

Die Unterscheidung zwischen statischen und dynamischen Vorschriften ist für die weitere Übertragbarkeit wichtig. Denn abhängig davon müssen entsprechende Modifikationen an dem Lösungsvorschlag vorgenommen werden.

### D. Übertragbarkeit des Prüfungsablaufs

Der grundlegende Prüfungsablauf, wie er für die datenverarbeitenden TOM dargestellt wurde,<sup>2</sup> sollte auch auf andere Bereiche übertragbar sein. Die Prüfung sollte daher ihren Ausgangspunkt bei der Sicherheit der Verarbeitung haben, da es auch bei anderen, rechtlich fragwürdigen TOM um einzelne Maßnahmen geht, die in den ersten Schritten keine Auswirkungen auf den Prüfungsablauf der Sicherheit der Verarbeitung haben. Wie oben auch, gilt es daher das Risiko der Verarbeitung zu bestimmen und anschließend eine Bestandsaufnahme der technischen und organisatorischen Maßnahmen vorzunehmen.

Nachdem dies erfolgt ist, kommt es zur Bewertung der Maßnahmen. Anders als oben werden hier im Rahmen des Abwägungskriteriums der allgemeinen „rechtlichen Bewertung“ die einschlägigen Rechtsvorschriften bewertet. Ebenfalls erfolgt eine Bewertung der TOM anhand der Kriterien „Stand der Technik“ und „Implementierungskosten“. Nach erfolgter Bewertung sollten die TOM auch wieder in eine entsprechende Implementierungsreihenfolge gebracht werden. An dieser Stelle wirkt sich dann die Differenzierung nach statischen und dynamischen Regulierungsvorschriften aus.

Kommt die Bewertung bei statischen Vorschriften zu dem Ergebnis, dass die TOM gegen das Recht verstoßen und nicht implementiert werden dürfen, wirkt die Bewertung hier absolut. Es besteht keine Möglichkeit, dieses Verbot mit den anderen Abwägungskriterien aufzuwiegen. Die betroffenen TOM müssen daher aus der weiteren Betrachtung herausgenommen werden. Sie sind so zu behandeln, als würde es sie nicht geben.

Bei dynamischen Vorschriften ist die Auflösung des Spannungsverhältnisses schwieriger. Denn hier kommt es darauf an, welche Wertungen hinter der entsprechenden Vorschrift und deren Bewertung der TOM stehen. Anhand dieser Wertungen muss versucht werden, den Ausgleich vorzunehmen. Dies kann be-

---

<sup>2</sup> Siehe hierzu: Kap. 12 *Prüfungsablauf*.



sonders dort eine Herausforderung darstellen, wo keine gemeinsamen Anknüpfungspunkte zwischen der Sicherheit der Verarbeitung und der einschlägigen Vorschrift bestehen. Im Falle der datenverarbeitenden TOM war dies noch relativ leicht, denn die Wertungen und darauf gerichteten Instrumente ließen sich z.T. miteinander kombinieren. Erlaubt die Vorschrift einen entsprechenden Ausgleich, dann kann ähnlich wie bei den datenverarbeitenden TOM auf dieser Basis eine Implementierungsreihenfolge aufgebaut werden. Anschließend kann dann anhand dieser Reihenfolge geprüft werden, welches Schutzniveau angemessen für das bestehende Risiko ist und damit welche Maßnahmen implementiert werden sollen. Sollten jedoch keine Instrumente bestehen, die einen solchen Ausgleich zulassen, bedarf es wohl einer Überarbeitung des Lösungsvorschlags, der auf die Besonderheiten der jeweiligen Rechtsvorschriften abgestimmt ist.

## E. Zwischenergebnis

Der hier dargestellte Lösungsvorschlag ist nicht auf das Problem datenverarbeitender TOM beschränkt. In weiten Teilen lassen sich die erarbeiteten Ansätze auch auf andere Bereiche innerhalb der Rechtsordnung übertragen, wo gesonderte Anforderungen an die Implementierung von technischen und organisatorischen Maßnahmen gestellt werden. Dabei ist vor allem das System der jeweiligen Regulierungsvorschriften zu beachten.

Handelt es sich um statische Vorschriften, die nur das Verbot von TOM kennen, fällt die Bewertung recht kurz aus. Bei einem absoluten Verbot der TOM dürfen diese nicht in die nähere Betrachtung aufgenommen werden. Sie werden so behandelt, als gäbe es sie nicht.

Problematischer sind hingegen dynamische Vorschriften, die wie das Datenschutzrecht einer Implementierung der TOM kritisch gegenüberstehen, deren Verbot aber an weitere Anforderungen knüpfen. Die Herausforderung besteht hier vor allem darin zu prüfen, ob der vorgestellte Lösungsvorschlag auf dieses System anwendbar ist. Im schlimmsten Fall bedarf es einer Anpassung der Lösung, an die Besonderheiten der einschlägigen Vorschriften.



## Schlussthesen

Abschließend lassen sich die, im 1. Teil dieser Arbeit gestellten Forschungsfragen wie folgt beantworten:

### *1. Forschungsfrage:*

Welche Folgen hat es auf die Sicherheit der Verarbeitung, wenn der Einsatz von bestimmten technischen und organisatorischen Maßnahmen an andere rechtliche Voraussetzungen (wie die Anforderungen an eine rechtmäßige Datenverarbeitung) geknüpft wird und die Gefahr eines Verbots dieser Maßnahmen besteht?

1. Die Sicherheit der Verarbeitung dient dem Schutz der betroffenen Personen<sup>1</sup> vor einem personal data breach i.S.d. Art. 4 Nr. 12 DS-GVO<sup>2</sup> bei Verarbeitung ihrer personenbezogenen Daten.
2. Allgemein gültige Anforderungen an die damit zu gewährleistende Sicherheit der Verarbeitung stellt die Verordnung nicht. Die Anforderungen richten sich vielmehr nach dem Risiko der jeweiligen Verarbeitung und sind am Einzelfall zu bestimmen.<sup>3</sup>
3. Gleichzeitig verlangt die Verordnung aber auch keinen absoluten Schutz, der das Risiko für die Verarbeitung vollständig begegnet. Datenverarbeitender müssen ein, dem Risiko angemessenes Schutzniveau gewährleisten. Die Vorschrift folgt damit dem Gebot der Verhältnismäßigkeit.<sup>4</sup>

---

<sup>1</sup> Siehe hierzu: Kap. 4, B. *Schutz der Rechte und Freiheiten* und Kap. 4, D. *Einschränkung auf das Risiko für betroffene Personen*.

<sup>2</sup> Siehe hierzu: Kap. 4, C. *Personal data breaches (und andere Sicherheitsvorfälle)* und dort insb. III. *Anwendung auf (andere) Sicherheitsvorfälle*.

<sup>3</sup> Siehe hierzu: Kap. 5, A. *Risikobewertung*.

<sup>4</sup> Siehe hierzu: Kap. 5, B., I. *Bedeutung der Angemessenheit*.

4. Die Angemessenheit des Schutzniveaus bestimmt sich im Rahmen einer Abwägung (mindestens) anhand der Kriterien Stand der Technik, Implementierungskosten, einem Verarbeitungskriterium und dem Risiko für die Rechte und Freiheiten betroffener Personen.<sup>5</sup>
5. Die Umsetzung des angemessenen Schutzniveaus erfolgt anschließend durch die Implementierung von technischen und organisatorischen Maßnahmen.<sup>6</sup>
6. Die Datenschutz-Grundverordnung kennt mit der Konkretisierung der Maßnahmen „technischer und organisatorischer Art“<sup>7</sup>, ihrer „Geeignetheit“<sup>8</sup> und einer „Auflistung von Aspekten, über die die Maßnahmen verfügen müssen“<sup>9</sup> zwar mehrere Anzeichen für gesetzliche Vorgaben, die bei der Implementierung zu beachten sind. Hierbei handelt es sich allerdings nicht um „harte“ Vorgaben, die zu einer nennenswerten Einschränkung führen, sondern eher um Orientierungshilfen. Grundsätzlich dienen die Maßnahmen als Mittel zum Zweck und gesetzliche Vorgaben an die Maßnahmen könnten dann diesem Zweck schaden.<sup>10</sup>
7. Dies bedeutet gleichzeitig, dass die Datenschutz-Grundverordnung keine Pflicht kennt, bestimmte (datenverarbeitende) TOM zu implementieren.<sup>11</sup> Dies löst allerdings nicht den beschriebenen Konflikt. Denn faktisch können Datenverarbeiter weiterhin gezwungen sein, datenverarbeitende TOM zu implementieren, wenn andernfalls nicht das geforderte Schutzniveau gewährleistet werden kann.<sup>12</sup> Zudem führt ein

---

<sup>5</sup> Siehe hierzu: Kap. 5, B., III. *Art. 32 Abs. 1 Hs. 1 DS-GVO als Abwägungskriterien der Angemessenheit?*

<sup>6</sup> Siehe hierzu: Kap. 5, C., I. *Allgemeines*.

<sup>7</sup> Siehe hierzu: Kap. 5, C., II. *Technischer und organisatorischer Art*.

<sup>8</sup> Siehe hierzu: Kap. 5, C., III. *Geeignetheit der Maßnahmen*.

<sup>9</sup> Siehe hierzu: Kap. 5, C., IV. *Anforderungen an die Maßnahmen nach Art. 32 Abs. 1 Hs. 2 DS-GVO*.

<sup>10</sup> Siehe hierzu: Kap. 5, C., V. *Telos als Basis gesetzgeberischer Vorgaben*.

<sup>11</sup> Siehe hierzu: Kap. 6, A., II. *Keine Pflicht zur Implementierung (datenverarbeitender) TOM*.

<sup>12</sup> Siehe hierzu: Kap. 6, C., I. *„Pflicht“ zur Implementierung bestimmter (datenverarbeitender) TOM*.

nachträgliches Verbot von technischen und organisatorischen Maßnahmen zu einer Verzerrung der Angemessenheitsprüfung und dem damit verbundenen Gebot der Verhältnismäßigkeit.<sup>13</sup>

8. Im Falle einer möglichen Berücksichtigung der datenschutzrechtlichen Bewertung von TOM ist allerdings zu beachten, dass zwischen der Sicherheit im Allgemeinen und einzelnen Sicherheitsmaßnahmen differenziert werden muss.<sup>14</sup> Eine Berücksichtigung muss daher im Rahmen der Angemessenheitsprüfung erfolgen.<sup>15</sup>
9. Eine Subsumtion der datenschutzrechtlichen Bewertung von TOM unter die Kriterien des „Stand der Technik“<sup>16</sup>, den „Implementierungskosten“<sup>17</sup>, dem „Verarbeitungskriterium“<sup>18</sup> und dem „Risiko für die Rechte und Freiheiten betroffener Personen“<sup>19</sup> ist nicht möglich.<sup>20</sup>
10. Rechtspolitisch wäre die Berücksichtigung der datenschutzrechtlichen Bewertung von TOM allerdings mit Blick auf die (bereits bestehenden) Abwägungskriterien und deren Funktion angebracht.<sup>21</sup>
11. Die Kriterien zur Bestimmung der Angemessenheit nach Art. 32 Abs. 1 Hs. 1 DS-GVO müssen im Zusammenhang mit Art. 32 Abs. 2 DS-GVO gelesen werden. Dieser enthält eine nicht abschließende Aufzählung für die Bestimmung des angemessenen Schutzniveaus.<sup>22</sup>

---

<sup>13</sup> Siehe hierzu: Kap. 6, C., III. *Gefahr einer Verzerrung der Angemessenheit*.

<sup>14</sup> Siehe hierzu: Kap. 7, A., I. *Zwingende Differenzierung zwischen Sicherheit und Sicherheitsmaßnahmen*.

<sup>15</sup> Siehe hierzu: Kap. 7, A., II. *Datenverarbeitende TOM als Teil der Angemessenheitsprüfung*.

<sup>16</sup> Siehe hierzu: Kap. 7, B., I. *Stand der Technik*.

<sup>17</sup> Siehe hierzu: Kap. 7, B., II. *Implementierungskosten*.

<sup>18</sup> Siehe hierzu: Kap. 7, B., III. *Verarbeitungskriterium*.

<sup>19</sup> Siehe hierzu: Kap. 7, B., IV. *Risiko für die Rechte und Freiheiten betroffener Personen*.

<sup>20</sup> Siehe hierzu: Kap. 7, B., V. *Systematisierung und Zwischenergebnis*.

<sup>21</sup> Siehe hierzu: Kap. 7, C., I. *Ein Kriterium der datenschutzrechtlichen Bewertung von TOM im Lichte der Abwägung des Art. 32 DS-GVO*.

<sup>22</sup> Siehe hierzu: Kap. 7, C., II., 2., c) *Offene Aufzählung der (äußeren) ersten Ebene*.

12. Im Rahmen dieser nicht abschließenden Aufzählung ist im Wege der Auslegung (oder hilfsweise mittels einer teleologischen Reduktion)<sup>23</sup> die datenschutzrechtliche Bewertung von TOM als weiteres Kriterium bei der Abwägung zu berücksichtigen.<sup>24</sup>
13. Inhaltlich umfasst dieses Kriterium nicht nur die Extremfälle, also ob die, den technischen und organisatorischen Maßnahmen zugrundeliegende Datenverarbeitung verboten ist oder nicht. Auch der Bereich dazwischen, i.S.e. datenschutzrechtlichen Bedenklichkeit hinsichtlich der TOM lässt sich mit dem Kriterium berücksichtigen.<sup>25</sup>
14. Zusammenfassend lässt sich die 1. Forschungsfragen dahingehend beantworten, dass die datenschutzrechtliche Bewertung von TOM im Rahmen der Angemessenheit des Schutzniveaus berücksichtigt werden kann und somit mit über die Anforderungen an die Sicherheit der Verarbeitung entscheidet.

## 2. Forschungsfrage:

Privilegiert die Klassifizierung als Maßnahme i.S.d. Sicherheit der Verarbeitung nach Art. 32 DS-GVO die Entscheidung über die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DS-GVO?

15. Im europäischen Datenschutzrecht muss jede Verarbeitung personenbezogener Daten auf einer Rechtsgrundlage basieren.<sup>26</sup>
16. Welche Rechtsgrundlage einschlägig ist, richtet sich dabei nach dem Zweck der Verarbeitung.<sup>27</sup>

---

<sup>23</sup> Siehe hierzu: Kap. 7, C., II., 4. *Alternative: Die datenschutzrechtliche Bewertung von TOM als unbenannter Abwägungstatbestand im Wege einer teleologischen Reduktion.*

<sup>24</sup> Siehe hierzu: Kap. 7, C., II., 3. *Die datenschutzrechtliche Bewertung von TOM als unbenannter Abwägungstatbestand durch Auslegung der offenen Aufzählung.*

<sup>25</sup> Siehe hierzu: Kap. 7, C., III. *Konkretisierung des ungeschriebenen Abwägungskriteriums der datenschutzrechtlichen Bewertung von TOM.*

<sup>26</sup> Siehe hierzu: Kap. 2, A., II. *Die datenschutzrechtliche Vorabkontrolle nach Art. 6 DS-GVO und Kap. 8, A. Die Notwendigkeit einer Rechtsgrundlage.*

<sup>27</sup> Siehe hierzu: Kap. 8, B. *Ausrichtung am Zweck der Verarbeitung.*

17. Im Falle der Einwilligung als Rechtsgrundlage für die Verarbeitung muss der Zweck in der Einwilligung festgelegt sein.<sup>28</sup>
18. Stützt sich die Verarbeitung auf eine gesetzliche Rechtsgrundlage, grenzt das Gesetz den Anwendungsbereich der verschiedenen Rechtsgrundlagen durch die Definition eines Zweckrahmens ein.<sup>29</sup>
19. Der Zweckrahmen dient dem Gedanken, dass der Schutz vor einer Verarbeitung personenbezogener Daten nicht absolut ist und diesem ebenfalls schützenswerte Interessen entgegenstehen können.<sup>30</sup> Dabei kennt die Datenschutz-Grundverordnung verschiedene Instrumente, um diese entgegenstehenden Interessen zu identifizieren und die vorgegebenen Zweckrahmen weiter einzugrenzen.<sup>31</sup>
20. Zu unterscheiden ist hier zwischen drei Formen der Rechtsgrundlagen. Die „vollkommene Rechtsgrundlage“ legt das Interesse und damit den Zweckrahmen in der Datenschutz-Grundverordnung final fest.<sup>32</sup> Die „ergänzungsbedürftige Rechtsgrundlage“ erfordert eine ergänzende Rechtsgrundlage, mit der der Gesetzgeber dieser ergänzenden Rechtsgrundlage das Interesse und den Zweckrahmen weiter konkretisiert.<sup>33</sup> Abschließend gibt es noch die „abwägende Rechtsgrundlage“, die mithilfe einer Interessenabwägung eine Konkretisierung durch den Verantwortlichen verlangt.<sup>34</sup>
21. Datenverarbeitende TOM i.S.d. Art. 32 DS-GVO bedürfen nach dem Prinzip des europäischen Datenschutzrechts ebenfalls einer Rechtsgrundlage für ihre Verarbeitung.<sup>35</sup>

---

<sup>28</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen.*

<sup>29</sup> Siehe hierzu: Kap. 8, B., II. *Der Zweck innerhalb der Rechtsgrundlagen.*

<sup>30</sup> Siehe hierzu: Kap. 8, C., III., 1. *Die gesetzlichen Rechtsgrundlagen als Ausdruck einer Grundrechtsabwägung.*

<sup>31</sup> Siehe hierzu: Kap. 8, C., III., 2. *Verwirklichung der Abwägung.*

<sup>32</sup> Siehe hierzu: Kap. 8, C., III., 2., a) *Vollkommene Rechtsgrundlagen.*

<sup>33</sup> Siehe hierzu: Kap. 8, C., III., 2., b) *Ergänzungsbedürftige Rechtsgrundlagen.*

<sup>34</sup> Siehe hierzu: Kap. 8, C., III., 2., c) *Abwägende Rechtsgrundlage.*

<sup>35</sup> Siehe hierzu: Kap. 9 *Rechtsgrundlage für datenverarbeitende TOM.*

22. Die Sicherheit der Verarbeitung i.S.d. Art. 32 DS-GVO stellt nicht den Zweck der Verarbeitung dar, sondern bildet einen Zweckrahmen.<sup>36</sup>
23. Die Einordnung des Art. 32 DS-GVO als ergänzende Rechtsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) i.V.m. Abs. 3 DS-GVO scheidet daher aus, weil es an dem erforderlichen Zweck in Art. 32 DS-GVO mangelt.<sup>37</sup>
24. Auch die Einwilligung scheidet (faktisch) als Rechtsgrundlage für datenverarbeitende TOM aus, da der Verantwortliche die Datenverarbeitung in diesem Fall nicht von der Entscheidung der betroffenen Person abhängig machen kann.<sup>38</sup>
25. Ansonsten kommt der Frage nach einer einschlägigen Rechtsgrundlage für datenverarbeitende TOM allerdings eine nachrangige Bedeutung zu und kann am Einzelfall entschieden werden.<sup>39</sup>
26. Durch die Einschränkung auf die gesetzlichen Rechtsgrundlagen kommt damit deren gemeinsamer Tatbestand der Erforderlichkeit eine besondere Bedeutung zu.<sup>40</sup>
27. Der Tatbestand dient als Bindeglied zwischen der Datenverarbeitung und ihrem Zweck.<sup>41</sup>
28. Gleichzeitig ist der Tatbestand europäisch autonom und für alle gesetzlichen Rechtsgrundlagen einheitlich auszulegen.<sup>42</sup>
29. Inhaltlich handelt es sich bei der Erforderlichkeit um eine Abwägung zwischen dem Schutz vor einer Verarbeitung und dem Interesse an der Verarbeitung. Dabei kann es hilfreich sein, sich die Frage zu stellen, welche zumutbaren Alternativen zur Datenverarbeitung bestehen und wie effektiv der Zweck erreicht werden soll.<sup>43</sup>

---

<sup>36</sup> Siehe hierzu: Kap. 9, A. *Die Sicherheit der Verarbeitung als Verarbeitungszweck?*.

<sup>37</sup> Siehe hierzu: Kap. 9, B., II. *Anforderungen an den Zweck der Verarbeitung*.

<sup>38</sup> Siehe hierzu: Kap. 9, C., III. *Die Untauglichkeit der Einwilligung*.

<sup>39</sup> Siehe hierzu: Kap. 9, D. *Zwischenergebnis*.

<sup>40</sup> Siehe hierzu: Kap. 10, A. *Der Tatbestand im System der Rechtsgrundlagen*.

<sup>41</sup> Siehe hierzu: Kap. 10, B. *Bezugspunkte des Tatbestands*.

<sup>42</sup> Siehe hierzu: Kap. 10, C. *Autonome, übergreifende Auslegung*.

<sup>43</sup> Siehe hierzu: Kap. 10, D. *Auslegung der Erforderlichkeit*.



30. Auf die zweite Forschungsfrage ist daher zusammenfassend zu antworten, dass in der Sicherheit der Verarbeitung zwar nicht der unmittelbare Zweck der Verarbeitung verkörpert ist, allerdings dessen übergeordneter Zweckrahmen. Indem die Datenschutz-Grundverordnung die Rechtmäßigkeit vom Zweck der Verarbeitung abhängig macht und vor allem im Rahmen des Tatbestands der Erforderlichkeit eine Abwägung zwischen der Datenverarbeitung und ihrem Zweck vornimmt, ist damit auch der Einsatzzweck datenverarbeitender TOM als Mittel zur Gewährleistung der Sicherheit der Verarbeitung berücksichtigen.

### 3. Forschungsfrage:

Wie sieht eine gerechte Lösung des Spannungsverhältnisses zwischen beiden Vorschriften unter Berücksichtigung der Ergebnisse zu den Fragen 1 und 2 aus?

31. Die rechtliche Analyse der jeweiligen Regelungsbereiche zeigt eine Wechselwirkung zwischen den Anforderungen an die Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle im Zusammenhang datenverarbeitender TOM, die bei der Formulierung eines Lösungsvorschlags berücksichtigt werden muss.<sup>44</sup>
32. Eine gerechte Lösung muss daher beide Regelungsbereiche gleichermaßen berücksichtigen und i.S.e. Art „praktischen Konkordanz“ einen angemessenen Ausgleich schaffen.<sup>45</sup>
33. Die wesentlichen Instrumente für diesen Ausgleich sind, auf Seiten der Sicherheit der Verarbeitung das Abwägungskriterium der datenschutzrechtlichen Bewertung von TOM und auf Seiten der datenschutzrechtlichen Vorabkontrolle der Tatbestand der Erforderlichkeit.<sup>46</sup>
34. Der entscheidende Ansatzpunkt für den Ausgleich beider Regelungsbereiche liegt dabei in der Frage nach zumutbaren, alternativen, techni-

---

<sup>44</sup> Siehe hierzu: Kap. 10, E., II. *Wechselwirkung zwischen der Sicherheit der Verarbeitung und der datenschutzrechtlichen Vorabkontrolle.*

<sup>45</sup> Siehe hierzu: Kap. 11, B., I. *Grundlage.*

<sup>46</sup> Siehe hierzu: Kap. 11, B., II. *Instrumente.*

schen und organisatorischen Maßnahmen. Denn hiermit lassen sich sowohl Aussagen über die Angemessenheit des Schutzniveaus als auch über die Erforderlichkeit einer möglichen Datenverarbeitung im Rahmen von datenverarbeitenden TOM treffen.<sup>47</sup>

35. Für die praktische Umsetzung des Lösungsansatzes wird ein Prüfungsschema vorgeschlagen, das seinen Anfang bei der Ermittlung des angemessenen Schutzniveaus nach Art. 32 DS-GVO nimmt und in dem dann die Prüfung der Erforderlichkeit einer Datenverarbeitung integriert wird.<sup>48</sup>
36. Das Prüfungsschema setzt sich zusammen aus der „Identifikation und Bewertung des Risikos der Verarbeitung“<sup>49</sup>, einer „Bestandsaufnahme geeigneter TOM“<sup>50</sup>, der „Bewertung der TOM“<sup>51</sup>, der Festlegung einer „Implementierungsreihenfolge“<sup>52</sup>, der daran anknüpfenden „Ableitung des angemessenen Schutzniveaus“<sup>53</sup> und zuletzt einer „laufenden Kontrolle dieses Schutzniveaus“<sup>54</sup>.
37. Für den Ausgleich der beiden Regelungsbereiche ist dabei zunächst die Bewertung der TOM entscheidend, bei der neben den anderen Aufwandskriterien auch die datenschutzrechtliche Bewertung der TOM und damit deren Auswirkungen auf den Datenschutz der betroffenen Personen berücksichtigt wird.<sup>55</sup>
38. Mit der anschließenden Implementierungsreihenfolge soll – im Verhältnis zu den anderen Aufwandskriterien – den TOM der Vorzug gewährt werden, die datenschutzrechtlich unbedenklicher sind. Erst wenn sich das Risiko mit diesen Maßnahmen nicht angemessen begegnen lässt, soll

---

<sup>47</sup> Siehe hierzu: Kap. 11, B., III., 2. *Die Bedeutung alternativer TOM.*

<sup>48</sup> Siehe hierzu: Kap. 11, C. *Praktische Umsetzung des Lösungsansatzes.*

<sup>49</sup> Siehe hierzu: Kap. 12, A. *Identifikation und Bewertung des Risikos der Verarbeitung.*

<sup>50</sup> Siehe hierzu: Kap. 12, B. *Bestandsaufnahme geeigneter TOM.*

<sup>51</sup> Siehe hierzu: Kap. 12, C. *Bewertung der TOM.*

<sup>52</sup> Siehe hierzu: Kap. 12, D. *Festlegung einer „Implementierungsreihenfolge“.*

<sup>53</sup> Siehe hierzu: Kap. 12, E. *Ableitung des angemessenen Schutzniveaus.*

<sup>54</sup> Siehe hierzu: Kap. 12, F. *Überprüfung des angemessenen Schutzniveaus.*

<sup>55</sup> Siehe hierzu: Kap. 12, C. *Bewertung der TOM.*

auf datenintensivere Maßnahmen zurückgegriffen werden, um dem dann verstärkten Interesse an der Verarbeitung gerecht zu werden.<sup>56</sup>

39. Auf die dritte Forschungsfrage ist daher zusammenfassend zu antworten, dass sich mit dem hier vorgeschlagenen Prüfungsschema<sup>57</sup> das Spannungsverhältnisses zwischen beiden Vorschriften unter Berücksichtigung der identifizierten Instrumente aus diesen Vorschriften gerecht lösen lässt.
40. Ergänzendes, über die Fragestellung hinausgehendes Ergebnis ist, dass die hier erarbeitete Lösung nicht nur das Problem datenverarbeitender TOM lösen kann, sondern darüber hinaus auch Erkenntnisse und Lösungsansätze für sämtliche TOM liefert, an deren Implementierung die Rechtsordnung besondere Anforderungen stellt. Abhängig von den jeweiligen Vorschriften muss die Lösung allerdings angepasst werden.<sup>58</sup>

---

<sup>56</sup> Siehe hierzu: Kap. 12, D. *Festlegung einer „Implementierungsreihenfolge“*.

<sup>57</sup> Siehe hierzu: Kap. 12 *Prüfungsablauf*.

<sup>58</sup> Siehe hierzu: Kap. 14 *Übertragbarkeit der Lösung*.



## Literaturverzeichnis

- Adrian, Axel*, Grundprobleme einer juristischen (gemeinschaftsrechtlichen) Methodenlehre, Berlin 2009 (zit.: *Adrian*, Grundprobleme einer juristischen (gemeinschaftsrechtlichen) Methodenlehre, 2009).
- Albers, Marion*, Informationelle Selbstbestimmung, Baden-Baden 2005 (zit.: *Albers*, Informationelle Selbstbestimmung, 2005).
- Albrecht, Jan Philipp*, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung – Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, in: *Computer und Recht* 2016, S. 88-98 (zit.: *Albrecht*, CR 2016, S. 88).
- Albrecht, Jan Philipp/Jotzo, Florian*, Das neue Datenschutzrecht der EU, Baden-Baden 2017, (zit.: *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017).
- Alt, Ulrich*, Datensicherheit, Datenschutz und Technik – ein risikoorientierter Ansatz, in: *Die Sachverständigen* 2020, S. 169-172, (zit.: *Alt*, DS 2020, S. 169).
- Anweiler, Jochen*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, Frankfurt a.M. 1997, (zit.: *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997).
- Arthur, W. Brian*, Competing Technologies, Increasing Returns, and Lock-In by Historical Events, in: *The Economic Journal* 1989, Volume 99, pp. 116-131, (zit.: *Arthur*, *The Economic Journal* Vol. 99 (1989), p. 116).
- Arthur, W. Brian* [Ed.], Increasing returns and path dependence in the economy, Ann Arbor 1994, (zit.: *Arthur* [Ed.], Increasing returns and path dependence in the economy, 1994).
- Auer-Reinsdorff, Astrid/Conrad, Isabell* [Hrsg.], Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019, (zit.: *Auer-Reinsdorff/Conrad/Bearbeiter*, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019).
- Auernhammer*, DSGVO BDSG, Kommentar, 8. Auflage, Hürth 2024, (zit.: *Auernhammer/Bearbeiter*, 8. Aufl. 2024).

- Barnes, William/Gartland, Myles/Stack, Martin*, Old Habits Die Hard: Path Dependency and Behavioral Lock-In, in: *Journal of Economic Issues* 2004, Volume 38, pp. 371-377, (zit.: *Barnes/Gartland/Stack*, JEI Vol. 38 (2004), p. 371).
- Bartels, Karsten U./Backer, Merlin*, Die Berücksichtigung des Stands der Technik in der DSGVO – Neue Anforderungen an die IT-Sicherheit im Datenschutz, in: *Datenschutz und Datensicherheit* 2018, S. 214-219, (zit.: *Bartels/Backer*, DuD 2018, S. 214).
- Beck, Gunnar*, *The Legal Reasoning of the Court of Justice of the EU*, London 2012, (zit.: *Beck*, *The Legal Reasoning of the Court of Justice of the EU*, 2012).
- Beck'scher Online-Kommentar BGB, Kommentar, Stand: 68. Edition, München 2023, (zit.: *BeckOK BGB/Bearbeiter*, Stand: 68. Ed. 2023).
- Beck'scher Online-Kommentar Datenschutzrecht, Kommentar, Stand: 45. Edition, München 2023, (zit.: *BeckOK Datenschutzrecht/Bearbeiter*, Stand: 46. Ed. 2023)
- Becker, Frank*, Meldungen nach Art. 33 DS-GVO – Voraussetzungen der Meldepflicht und die Doppelrolle der Aufsichtsbehörden, in: *Zeitschrift für Datenschutz* 2020, S. 175-179, (zit.: *Becker*, ZD 2020, S. 175).
- Bieker, Felix*, Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, in: *Datenschutz und Datensicherheit* 2018, S. 27-31, (zit.: *Bieker*, DuD 2018, S. 27).
- Bieker, Felix/Bremert, Benjamin*, Identifizierung von Risiken für die Grundrechte von Individuen – Auslegung und Anwendung des Risikobegriffs der DS-GVO, in: *Zeitschrift für Datenschutz* 2020, S. 7-14, (zit.: *Bieker/Bremert*, ZD 2020, S. 7).
- Bieker, Felix/Bremert, Benjamin/Hansen, Marit*, Die Risikobeurteilung nach der DSGVO, in: *Datenschutz und Datensicherheit* 2018, S. 492-496, (zit.: *Bieker/Bremert/Hansen*, DuD 2018, S. 492).
- Bieker, Felix/Hansen, Marit/Friedewald, Michael*, Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, in: *Recht der Datenverarbeitung* 2016, S. 188-197, (zit.: *Bieker/Hansen/Friedewald*, RDV 2016, S. 188).
- Bleckat, Alexander*, Abdingbarkeit des Art. 32 DS-GVO durch Einwilligung, in: *Recht der Datenverarbeitung* 2021, S. 206-208, (zit.: *Bleckat*, RDV 2021, S. 206).

- Boehme-Neßler, Volker*, Das Ende der Anonymität – Wie Big Data das Datenschutzrecht verändert, in: *Datenschutz und Datensicherheit* 2016, S. 419-423, (zit.: *Boehme-Neßler*, DuD 2016, S. 419).
- Brams, Isabelle*, Bußgeldrisiken nach Datenschutzvorfällen – Rechtlicher Rahmen – Aktuelle Bußgeldpraxis – Verteidigungsstrategien, in: *Zeitschrift für Datenschutz* 2023, S. 484-488, (zit.: *Brams*, ZD 2023, S. 484).
- Breyer, Jonas*, Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-GVO, in: *Datenschutz und Datensicherheit* 2018, S. 311-317, (zit.: *Breyer*, DuD 2018, S. 311).
- Bronner, Pascal/Wiedemann, Fabian*, Rechtmäßigkeit der Datenverarbeitung bei wissenschaftlicher Forschung an staatlichen Hochschulen – Chancen und Grenzen der breiten Einwilligung und gesetzlicher Erlaubnistatbestände, in: *Zeitschrift für Datenschutz* 2023, S. 77-85, (zit.: *Bronner/Wiedemann*, ZD 2023, S. 77).
- Buchholtz, Gabriele*, Grundrechte und Datenschutz im Dialog zwischen Karlsruhe und Luxemburg, in: *Die Öffentliche Verwaltung* 2017, S. 837-845, (zit.: *Buchholtz*, DÖV 2017, S. 837).
- Buchmann, Johannes*, Einführung in die Kryptographie, 6. Auflage, Berlin und Heidelberg 2016, (zit.: *Buchmann*, Einführung in die Kryptographie, 6. Aufl. 2016).
- Buchner, Benedikt*, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, in: *Datenschutz und Datensicherheit* 2016, S. 155-161, (zit.: *Buchner*, DuD 2016, S. 155).
- Buck, Carsten*, Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, Frankfurt a.M. 1998, (zit.: *Buck*, Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, 1998).
- Bunte, Hermann-Josef* [Hrsg.], Kartellrecht, Kommentar, Band 2 Europäisches Kartellrecht, Vergaberecht (GWB) und Sonderbereiche, 14. Auflage, Hürth 2022, (zit.: *Bunte/Bearbeiter*, Kartellrecht, Bd. 2, 14. Aufl. 2022).
- Bussche, Axel Freiherr von dem/Voigt, Paul* [Hrsg.], Konzerndatenschutz, 2. Auflage, München 2019, (zit.: v.d. *Bussche/Voigt/Bearbeiter*, Konzerndatenschutz, 2. Aufl. 2019).
- Bydlinski, Franz*, Juristische Methodenlehre und Rechtsbegriffe, 2. Auflage, Wien 1991, (zit.: *Bydlinski*, Juristische Methodenlehre und Rechtsbegriffe, 2. Aufl. 1991).
- Byers, Philipp/Winkler, Manuela/Stelter, Stasy*, Zulässigkeit von biometrischen Kontrollen am Arbeitsplatz, in: *Neue Zeitschrift für Arbeitsrecht* 2023, S. 457-463, (zit.: *Byers/Winkler/Stelter*, NZA 2023, S. 457).

- Calliess, Christian/Ruffert, Matthias* [Hrsg.], Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 6. Auflage, München 2022, (zit.: *Calliess/Ruffert/Bearbeiter*, EUV/AEUV, 6. Aufl. 2022).
- Canaris, Claus-Wilhelm*, Die Feststellung von Lücken im Gesetz, 2. Auflage, Berlin 1983, (zit.: *Canaris*, Die Feststellung von Lücken im Gesetz, 2. Aufl. 1983).
- Cherng, Ming-Shiou*, Verbote mit Erlaubnisvorbehalt im Rechte der Ordnungsverwaltung, Münster, Hamburg, Berlin und London 2001, (zit.: *Cherng*, Verbote mit Erlaubnisvorbehalt im Rechte der Ordnungsverwaltung, 2001).
- Chibanguza, Kuuya/Kuß, Christian/Steeger, Hans* [Hrsg.], Künstliche Intelligenz, Baden-Baden 2022, (zit.: *Chibanguza/Kuß/Steeger/Bearbeiter*, Künstliche Intelligenz, 2022).
- Colneric, Ninon*, Auslegung des Gemeinschaftsrechts und gemeinschaftsrechtskonforme Auslegung, in: Zeitschrift für Europäisches Privatrecht 2005, S. 225-233, (zit.: *Colneric*, ZEuP 2005, S. 225).
- Cremer, Wolfram*, Praktische Konkordanz als grundrechtliche Kollisionsauflösungsregel – Einbebnung gesetzgeberischer Entscheidungsspielräume, in: Kment, Martin [Hrsg.]: Das Zusammenwirken von deutschem und europäischem Öffentlichem Recht – Festschrift für Hans D. Jarass zum 70. Geburtstag, S. 175-183, München 2015, (zit.: *Cremer*, Praktische Konkordanz als grundrechtliche Kollisionsauflösungsregel, in: FS Jarass, 2015, S. 175).
- Culik, Nicolai/Döpke, Christian*, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen – Analyse möglicher Auswirkungen der DS-GVO, in: Zeitschrift für Datenschutz 2017, S. 226-230, (zit.: *Culik/Döpke*, ZD 2017, S. 226).
- Dammann, Ulrich*, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, in: Zeitschrift für Datenschutz 2016, S. 307-314, (zit. *Dammann*, ZD 2016, S. 307).
- Dannecker, Gerhard/Fischer-Fritsch, Jutta*, Das EG-Kartellrecht in der Bußgeldpraxis, Köln u.a. 1989, (zit.: *Dannecker/Fischer-Fritsch*, Das EG-Kartellrecht in der Bußgeldpraxis, 1989).
- von Danwitz, Thomas*, Der Grundsatz der Verhältnismäßigkeit im Gemeinschaftsrecht, in: Europäisches Wirtschafts- und Steuerrecht 2003, S. 393-402, (zit.: *von Danwitz*, EWS 2003, S. 393).
- DatKomm, Kommentar, Stand: 76. Ergänzungslieferung, Wien 2023, (zit.: *DatKomm/Bearbeiter*, Stand: 76. EL. 2023).



- Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke* [Hrsg.], EU-DSGVO und BDSG, Kommentar, 2. Auflage, Frankfurt a.M. 2020, (zit.: *Däubler u.a./Bearbeiter*, EU-DSGVO und BDSG, 2. Aufl. 2020).
- Dauses, Manfred A./Ludwigs, Markus* [Hrsg.], Handbuch des EU-Wirtschaftsrechts, Band 1, Stand: 59. Ergänzungslieferung, München 2023, (zit.: *Dauses/Ludwigs/Bearbeiter*, Hdb. des EU-Wirtschaftsrechts, Bd. 1, Stand: 59. EL. 2023).
- David, Paul A.*, Clio and the Economics of QWERTY, in: *The American Economic Review* 1985, Volume 75, pp. 332-337, (zit.: *David*, AER Vol. 75 (1985), p. 332).
- Dehnert, Henning/Weber, Marc Philipp*, EU-Kommissionsentwurf: Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DS-GVO – Auswirkungen auf die Zusammenarbeit der europäischen Aufsichtsbehörden, in: *Zeitschrift für Datenschutz* 2023, S. 648-653, (zit.: *Dehnert/Weber*, ZD 2023, S. 648).
- Detterbeck, Steffen*, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 21. Auflage, München 2023, (zit.: *Detterbeck*, Allgemeines Verwaltungsrecht, 21. Aufl. 2023).
- Deusch, Florian/Eggendorfer, Tobias*, Intrusion Detection und DSGVO, in: *Taeger, Jürgen* [Hrsg.]: Rechtsfragen digitaler Transformationen – Gestaltungen digitaler Veränderungsprozesse durch Recht, S. 741-754, Edewecht 2018, (zit.: *Deusch/Eggendorfer*, Intrusion Detection und DSGVO, in: *Rechtsfragen digitaler Transformationen*, 2018, S. 741).
- Drewes, Stefan*, Dialogmarketing nach der DSGVO ohne Einwilligung der Betroffenen – Berechtigte Unternehmensinteressen bleiben maßgebliche Rechtsgrundlage, in: *Computer und Recht* 2016, S. 721-729, (zit.: *Drewes*, CR 2016, S. 721).
- Eckert, Claudia*, IT-Sicherheit, 11. Auflage, Berlin und Boston 2023, (zit.: *Eckert*, IT-Sicherheit, 11. Aufl. 2023).
- Ehmann, Eugen/Selmayr, Martin* [Hrsg.], Datenschutz-Grundverordnung, Kommentar, 2. Auflage, München 2018, (zit.: *Ehmann/Selmayr/Bearbeiter*, Datenschutz-Grundverordnung, 2. Aufl. 2018).
- Ernst, Stefan*, Die Widerruflichkeit der datenschutzrechtlichen Einwilligung – Folgen fehlender Belehrung und Einschränkungen, in: *Zeitschrift für Datenschutz* 2020, S. 383-385, (zit.: *Ernst*, ZD 2020, S. 383).
- Eusani, Guido*, Sachverständige und Datenschutz. Teil II – Praktische Umsetzung und Verstöße, in: *Die Sachverständigen* 2019, S. 18-30, (zit.: *Eusani*, DS 2019, S. 18).

*Feiler, Lukas/Forgó, Nikolaus*, EU-DSGVO und DSG, Kommentar, 2. Auflage, Wien 2022, (zit.: *Feiler/Forgó*, EU-DSGVO und DSG, 2. Aufl. 2022).

*Ferretti, Federico*, Data protection and the legitimate Interest of Data Controllers: much ado about nothing or the winter of rights?, in: *Common Market Law Review*, Volume 51, 2014, pp. 843-868, (zit.: *Ferretti*, CML Rev. 51 (2014), p. 843).

*Folkerts, Elena*, Datenschutzverletzungen in Abgrenzung zu unrechtmäßigen Datenverarbeitungen – Differenzierung und Konsequenzen, in: *Zeitschrift für Datenschutz* 2023, S. 654-658, (zit.: *Folkerts*, ZD 2023, S. 654).

*Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen* [Hrsg.], Betrieblicher Datenschutz, 3. Auflage, München 2019, (zit.: *Forgó/Helfrich/Schneider/Bearbeiter*, Betrieblicher Datenschutz, 3. Aufl. 2019).

*Franck, Lorenz*, Datensicherheit als datenschutzrechtliche Anforderung – Keine Abdingbarkeit technisch-organisatorischer Maßnahmen nach künftiger DSGVO? – zugleich Ergänzung zu Lotz/Wendler, CR 2016, 31 ff., in: *Computer und Recht* 2016, S. 238-240, (zit.: *Franck*, CR 2016, S. 238).

*Franzen, Martin*, Privatrechtsangleichung durch die Europäische Gemeinschaft, Berlin 1999, (zit.: *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999).

*Franzen, Martin*, Datenschutz-Grundverordnung und Arbeitsrecht, in: *Europäische Zeitschrift für Arbeitsrecht* 2017, S. 313-351, (zit.: *Franzen*, EuZA 2017, S. 313).

*Franzen, Martin/Gallner, Inken/Oetker, Hartmut* [Hrsg.], Kommentar zum europäischen Arbeitsrecht, 5. Auflage, München 2024, (zit.: *Franzen/Gallner/Oetker/Bearbeiter*, EuArbRK, 5. Aufl. 2024).

*Frenz, Walter*, Handbuch Europarecht, 4. Band Europäische Grundrechte, Berlin und Heidelberg 2009, (zit.: *Frenz*, Hdb. Europarecht, 4. Bd. Europäische Grundrechte, 2009).

*Freund, Bernhard/Schmidt, Bernd/Heep, Sebastian/Roschek, Anna-Kristina* [Hrsg.], DSGVO, Kommentar, Frankfurt a.M. 2023, (zit.: *Freund u.a./Bearbeiter*, DSGVO, 2023).

*Frisse, Florian/Glaßl, Ramón/Baranowski, Anne/Duwald, Lisa*, Unternehmenssicherheit bei Banken – IT-Sicherheit, Know-how Schutz, Datensicherheit und Datenschutz, in: *Zeitschrift für Bank- und Kapitalmarktrecht* 2018, S. 177-184, (zit.: *Frisse u.a.*, BKR 2018, S. 177).

*Fuhlbrott, Michael*, Data Incident Management: Rechtlicher Umgang mit „Datenpannen“, in: *Neue Zeitschrift für Arbeitsrecht* 2019, S. 649-653, (zit.: *Fuhlbrott*, NZA 2019, S. 649).

- Gärtner, Tanya/Selzer, Annika*, Angemessene technische und organisatorische Maßnahmen – Der ökonomische Balanceakt zwischen Kosten und Risiken, in: *Datenschutz und Datensicherheit* 2023, S. 289-594, (zit.: *Gärtner/Selzer*, DuD 2023, S. 289).
- Gebauer, Martin/Teichmann, Christoph* [Hrsg.], *Europäisches Privat- und Unternehmensrecht*, 2. Auflage, Baden-Baden 2022, (zit.: *Gebauer/Teichmann/Bearbeiter*, *Europäisches Privat- und Unternehmensrecht*, 2. Aufl. 2022).
- Gierschmann, Sibylle*, Was „bringt“ deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt, in: *Zeitschrift für Datenschutz* 2016, S. 51-55, (zit.: *Gierschmann*, ZD 2016, S. 51).
- Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried* [Hrsg.], *Datenschutz-Grundverordnung, Kommentar*, Köln 2018, (zit.: *Gierschmann u.a./Bearbeiter*, *Datenschutz-Grundverordnung*, 2018).
- Gola, Peter* [Hrsg.], *Datenschutz-Grundverordnung, Kommentar*, 1. Auflage, München 2017, (zit.: *Gola/Bearbeiter*, *Datenschutz-Grundverordnung*, 1. Aufl. 2017).
- Gola, Peter/Heckmann, Dirk* [Hrsg.], *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, Kommentar*, 3. Auflage, München 2022, (zit.: *Gola/Heckmann/Bearbeiter*, *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, 3. Aufl. 2022).
- Golla, Sebastian J./Hofmann, Henning/Bäcker, Matthias*, Connecting the Dots – Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu, in: *Datenschutz und Datensicherheit* 2018, S. 89-100, (zit.: *Golla/Hofmann/Bäcker*, DuD 2018, S. 89).
- Gossen, Heiko/Schramm, Marc*, Das Verarbeitungsverzeichnis der DS-GVO – Ein effektives Instrument zur Umsetzung der neuen unionsrechtlichen Vorgaben, in: *Zeitschrift für Datenschutz* 2017, S. 7-13, (zit.: *Gossen/Schramm*, ZD 2017, S. 7).
- Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin* [Hrsg.], *Das Recht der Europäischen Union*, Stand: 80. Ergänzungslieferung, München 2023, (zit.: *Grabitz/Hilf/Nettesheim/Bearbeiter*, *Das Recht der Europäischen Union*, Stand: 80. EL. 2023).
- von der Groeben, Hans/Schwarze, Jürgen/Hatje, Armin* [Hrsg.], *Europäisches Unionsrecht*, 7. Auflage, Baden-Baden 2015, (zit.: *von der Groeben/Schwarze/Hatje/Bearbeiter*, *Europäisches Unionsrecht*, 7. Aufl. 2015).
- Grundmann, Stefan*, »Inter-Instrumental-Interpretation« – Systembildung durch Auslegung im Europäischen Unionsrecht, in: *Rabels Zeitschrift für ausländisches und internationales Privatrecht* 2011, Band 75, S. 882-932, (zit.: *Grundmann*, *RabelsZ* 75 (2011), S. 882).

- Guckelberger, Annette*, Veröffentlichung der Leistungsempfänger von EU-Subventionen und unionsgrundrechtlicher Datenschutz, in: Europäische Zeitschrift für Wirtschaftsrecht 2011, S. 126-130, (zit.: *Guckelberger*, EuZW 2011, S. 126).
- Haas, Christoph/Kast, Christian R.*, Network Security Monitoring – Ein modernes Schutzsystem aus technischer und rechtlicher Sicht, in: Zeitschrift für Datenschutz 2015, S. 72-77, (zit.: *Haas/Kast*, ZD 2015, S. 72).
- Haase, Martin*, Die Einwilligung im Datenschutzrecht – Einschränkungen der Freiheit des Einzelnen durch die überzogene Forderung nach Freiwilligkeit, in: Zeitschrift zum Innovations- und Technikrecht, S. 113-118, (zit.: *Haase*, InTeR 2019, S. 113).
- Hager, Günter*, Rechtsmethoden in Europa, Tübingen 2009, (zit.: *Hager*, Rechtsmethoden in Europa, 2009).
- Hansen, Marit/Walczak, Benjamin*, Pseudonymisierung à la DS-GVO und verwandte Methoden, in: Recht der Datenverarbeitung 2019, S. 53-57, (zit.: *Hansen/Walczak*, RDV 2019, S. 53).
- Härtel, Ines*, Handbuch Europäische Rechtsetzung, Berlin und Heidelberg 2006, (zit.: *Härtel*, Hdb. Europäische Rechtsetzung, 2006).
- Härtling, Niko/Gössling, Patrick/Dimov, Vitorio*, „Berechtigte Interessen“ nach der DSGVO, in: IT-Rechtsberater 2017, S. 169-172, (zit.: *Härtling/Gössling/Dimov*, ITRB 2017, S. 169).
- Hauschka, Christoph E./Moosmayer, Klaus/Lösler, Thomas* [Hrsg.], Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 3. Auflage, München 2016, (zit.: *Hauschka/Moosmayer/Lösler/Bearbeiter*, Corporate Compliance, 3. Aufl. 2016).
- Heidrich, Joerg*, Stresstest für die DSGVO: Anatomie eines Daten-Gau, in: Taeger, Jürgen [Hrsg.]: Den Wandel begleiten – IT-rechtliche Herausforderungen der Digitalisierung, S. 391-404, Edewecht 2020, (zit.: *Heidrich*, Stresstest für die DSGVO, in: Den Wandel begleiten, 2020, S. 391).
- Heidrich, Joerg/Tschoepe, Sven*, Rechtsprobleme der E-Mail-Filterung, in: Multimedia und Recht 2004, S. 75-80, (zit.: *Heidrich/Tschoepe*, MMR 2004, S. 75).
- Heinzke, Philippe/Engel, Lennart*, Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen. Reichweite des Art. 6 Abs. 1 1. Unterabs. lit. b DS-GVO, in: Zeitschrift für Datenschutz 2020, S. 189-194, (zit.: *Heinzke/Engel*, ZD 2020, S. 189).
- Hellmann, Roland*, IT-Sicherheit, 2. Auflage, Berlin/Boston 2023, (zit.: *Hellmann*, IT-Sicherheit, 2. Aufl. 2023).

*Henninger, Thomas*, Europäisches Privatrecht und Methode, Tübingen 2009, (zit.: *Henninger*, Europäisches Privatrecht und Methode, 2009).

*Herfurth, Constantin*, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO – Nachvollziehbare Ergebnisse anhand von 15 Kriterien mit dem sog. „3x5-Modell“, in: Zeitschrift für Datenschutz 2018, S. 514-520, (zit.: *Herfurth*, ZD 2018, S. 514).

*Herresthal, Carsten*, Die teleologische Auslegung der Verbrauchsgüterkaufrichtlinie – Der EuGH auf dem Weg zu einer eigenständigen Methode der Rechtsgewinnung (zugleich Anmerkung des EuGH-Urteils, vom 17.04.2008, Rs. C-404/06 – Quelle), in: Zeitschrift für Europäisches Privatrecht 2009, S. 598-612, (zit.: *Herresthal*, ZEuP 2009, S. 598).

*Heselhaus, Sebastian M./Nowak, Carsten* [Hrsg.], Handbuch der Europäischen Grundrechte, 2. Auflage, München 2020, (zit.: *Heselhaus/Nowak/Bearbeiter*, Hdb. der Europäischen Grundrechte, 2. Aufl. 2020).

*Hesse, Konrad*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage, Heidelberg 1999, (zit.: *Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl. 1999).

*Hoeren, Thomas*, Virenscreening und Spamfilter – Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co., in: Neue Juristische Wochenschrift 2004, S. 3513-3517, (zit.: *Hoeren*, NJW 2004, S. 3513).

*Hoeren, Thomas/Sieber, Ulrich/Holznapel, Bernd* [Hrsg.], Handbuch Multimedia-Recht, Stand: 59. Ergänzungslieferung, München 2023, (zit.: *Hoeren/Sieber/Holznapel/Bearbeiter*, Hdb. Multimedia-Recht, Stand: 59. EL. 2023).

*Hoffmann, Bernhard*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes, Baden-Baden 1991, (zit.: *Hoffmann*, Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes, 1991).

*Hofmann, Johanna M./Johannes, Paul C.*, DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs – Begriffsklärung der entscheidenden Frage des sachlichen Anwendungsbereichs, in: Zeitschrift für Datenschutz 2017, S. 221-226, (zit.: *Hofmann/Johannes*, ZD 2017, S. 221).

*Höpfner, Clemens/Rüthers, Bernd*, Grundlagen einer europäischen Methodenlehre, in: Archiv für civilistische Praxis 2009, Band 209, S. 1-36, (zit.: *Höpfner/Rüthers*, AcP 209 (2009), S. 1).

*Hornung, Gerrit/Gilga, Carolin*, Einmal öffentlich – für immer schutzlos? Die Zulässigkeit der Verarbeitung öffentlicher personenbezogener Daten, in: Computer und Recht 2020, S. 367-379, (zit.: *Hornung/Gilga*, CR 2020, S. 367).

- Hornung, Gerrit/Schallbruch, Martin* [Hrsg.], IT- Sicherheitsrecht, Baden-Baden 2021, (zit.: *Hornung/Schallbruch/Bearbeiter*, IT-Sicherheitsrecht, 2021).
- Hufen, Friedhelm*, Staatsrecht II, 10. Auflage, München 2023, (zit.: *Hufen*, Staatsrecht II, 10. Aufl. 2023).
- Ihwas, Saleh R.*, Das neue Datenschutzstrafrecht – Bußgeldrisiken für Unternehmen nach der DSGVO und Strafbarkeitsrisiken für Individualpersonen nach dem BDSG, in: *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht* 2021, S. 289-296, (zit.: *Ihwas*, NZWiSt 2021, S. 289).
- Immenga, Ulrich/Mestmäcker, Ernst-Joachim* [Begr.], Wettbewerbsrecht, Kommentar, 1. Band Europäisches Kartellrecht, 6. Auflage, München 2019, (zit.: *Immenga/Mestmäcker/Bearbeiter*, Wettbewerbsrecht, 1. Bd., 6. Aufl. 2019).
- Ipsen, Jörn*, Allgemeines Verwaltungsrecht, 11. Auflage, München 2019, (zit.: *Ipsen*, Allgemeines Verwaltungsrecht, 11. Aufl. 2019).
- Jahnel, Dietmar* [Hrsg.], Datenschutz-Grundverordnung, Kommentar, Wien 2021, (zit.: *Jahnel/Bearbeiter*, DSGVO, 2021).
- Jahnel, Dietmar/Pallwein-Prettner, Angelika*, Datenschutzrecht, 3. Auflage, Wien 2021, (zit.: *Jahnel/Pallwein-Prettner*, Datenschutzrecht, 3. Aufl. 2021).
- Jandt, Silke*, Datenschutz durch Technik in der DS-GVO – Präventive und repressive Vorgaben zur Gewährleistung der Sicherheit der Verarbeitung, in: *Datenschutz und Datensicherheit* 2017, S. 562-566, (zit.: *Jandt*, DuD 2017, S. 562).
- Jandt, Silke/Steidle, Roland* [Hrsg.], Datenschutz im Internet, Baden-Baden 2018, (zit.: *Jandt/Steidle/Bearbeiter*, Datenschutz im Internet, 2018).
- Jarass, Hans D.*, Charta der Grundrechte der Europäischen Union, Kommentar, 4. Auflage, München 2021, (zit.: *Jarass*, Charta der Grundrechte der EU, 4. Aufl. 2021).
- Jauernig*, Bürgerliches Gesetzbuch, Kommentar, 19. Auflage, München 2023, (zit.: *Jauernig/Bearbeiter*, BGB, 19. Aufl. 2023).
- Johannes, Paul C./Gemin, Christian L.*, Abwägung zur Sicherheit der Datenverarbeitung durch technische und organisatorische Maßnahmen, in: *Zeitschrift zum Innovations- und Technikrecht*, S. 140-146, (zit.: *Johannes/Gemin*, InTeR 2021, S. 140).

- John, Nicolas/Schaller, Johanna*, Keine Disponibilität der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO – Eine kritische Auseinandersetzung mit dem Beschluss der DSK, in: *Computer und Recht* 2022, S. 156-159, (zit.: *John/Schaller*, CR 2022, S. 156).
- Joos, Daniel/Nägele, Peter*, Verarbeitung personenbezogener Echtdaten zur Netz- und Informationssicherheit – Softwaretestungen unter Berücksichtigung des Datenschutzes, in: *Datenschutz und Datensicherheit* 2022, S. 578-583, (zit.: *Joos/Nägele*, DuD 2022, S. 578).
- Jung, Alexander*, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO. Praktikable Ansätze für die Erfüllung ordnungsgemäßer Datenverarbeitung, in: *Zeitschrift für Datenschutz* 2018, S. 208-213, (zit.: *Jung*, ZD 2018, S. 208).
- Jung, Stefanie*, Spezifika der europäischen Methodenlehre, in: Clavora, Selena/Garber, Thomas [Hrsg.]: *Das Vorabentscheidungsverfahren in der Zivilgerichtsbarkeit*, S. 17-32, Wien und Graz 2014, (zit.: *Jung*, Spezifika der europäischen Methodenlehre, in: *Das Vorabentscheidungsverfahren in der Zivilgerichtsbarkeit*, 2014, S. 17).
- Jung, Stefanie/Krebs, Peter*, Die Vertragsverhandlung – Taktische, strategische und rechtliche Elemente, Wiesbaden 2016, (zit.: *Jung/Krebs*, *Die Vertragsverhandlung*, 2016).
- Jung, Stefanie/Krebs, Peter/Stiegler, Sascha* [Hrsg.], *Gesellschaftsrecht in Europa*, Baden-Baden 2019, (zit.: *Jung/Krebs/Stiegler/Bearbeiter*, *Gesellschaftsrecht in Europa*, 2019).
- Jungkind, Vera/Koch, Susanne*, The risk-based approach in the GDPR – Restating the obvious and reinstating a guiding principle, in: *Zeitschrift für Datenschutz* 2022, S. 656-664, (zit.: *Jungkind/Koch*, ZD 2022, S. 656).
- Junker, Abbo*, Systembildung und Systemlücken im harmonisierten Arbeitsvertragsrecht, in: *Neue Zeitschrift für Arbeitsrecht* 1999, S. 2-11, (zit.: *Junker*, NZA 1999, S. 2).
- Kasner, Olga*, Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO – Die richtige Vorgehensweise bei Datenpannen, in: *Privacy in Germany* 2019, S. 111-114, (zit.: *Kasner*, PinG 2019, S. 111).
- Katko, Peter* [Hrsg.], *Checklisten zur Datenschutz-Grundverordnung*, 2. Auflage, München 2023, (zit.: *Katko/Bearbeiter*, *Checklisten zur Datenschutz-Grundverordnung*, 2. Aufl. 2023).
- Keppeler, Lutz/Berning, Wilhelm*, Die Bußgeldrisiken nach Art. 83 der Datenschutz-Grundverordnung – auch ein Risiko für den Jahresabschluss?!, in: *Deutsches Steuerrecht* 2018, S. 91-96, (zit.: *Keppeler/Berning*, DStR 2018, S. 91).

- Kiparski, Gerd/Zirfas, Julia*, Hallo, wer bin ich? — DSGVO Bußgeld bei nicht ausreichender Kundenauthentifizierung in Call Centern, in: *Computer und Recht* 2021, S. 108-116, (zit.: *Kiparski/Zirfas*, CR 2021, S. 108).
- Kipker, Dennis-Kenji*, Monatliches Themen-Update aus den Bereichen Digitalisierung, Datenschutz & Cybersecurity, in: *Newsdienst Multimedia und Recht-Aktuell* 2020, 433456, (zit.: *Kipker*, MMR-Aktuell 2020, 433456).
- Kipker, Dennis-Kenji* [Hrsg.], *Cybersecurity*, 2. Auflage, München 2023, (zit.: *Kipker/Bearbeiter*, *Cybersecurity*, 2. Aufl. 2023).
- Kipker, Dennis-Kenji/Reusch, Philipp/Ritter, Steve* [Hrsg.], *Recht der Informationssicherheit*, München 2023, (zit.: *Kipker/Reusch/Ritter/Bearbeiter*, *Recht der Informationssicherheit*, 2023).
- Klaas, Arne*, Die datenschutzkonforme Weitergabe von Ermittlungsergebnissen aus internen Untersuchungen – Teil 1: Nationale Behörden, in: *Corporate Compliance* 2020, S. 256-265, (zit.: *Klaas*, CCZ 2020, S. 256).
- Klaas, Arne/Momsen, Carsten/Wybitul, Tim* [Hrsg.], *Datenschutzsanktionenrecht*, München 2023, (zit.: *Klaas/Momsen/Wybitul/Bearbeiter*, *Datenschutzsanktionenrecht*, 2023).
- Klein, David*, Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?, in: *Sprech-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian/Thomsen, Oliver* [Hrsg.]: *Festschrift für Jürgen Taeger*, S. 235-249, Frankfurt a.M. 2020, (zit.: *Klein*, *Zivilrechtlicher Datenschutz oder datenschutzrechtliches Zivilrecht?*, in: *FS Taeger*, 2020, S. 235).
- Klement, Jan Henrik*, Öffentliches Interesse an Privatheit – Das europäische Datenschutzrecht zwischen Binnenmarkt, Freiheit und Gemeinwohl, in: *Juristen Zeitung* 2017, S. 161-170, (zit.: *Klement*, JZ 2017, S. 161).
- Knopp, Michael*, Stand der Technik – Ein alter Hut oder eine neue Größe?, in: *Datenschutz und Datensicherheit* 2017, S. 663-666, (zit.: *Knopp*, DuD 2017, S. 663).
- Knyrim, Rainer* [Hrsg.], *Praxishandbuch Datenschutzrecht*, 4. Auflage, Wien 2020, (zit.: *Knyrim/Bearbeiter*, *Praxishandbuch Datenschutzrecht*, 4. Aufl. 2020).
- Koch, Oliver*, *Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften*, Berlin 2003, (zit.: *Koch*, *Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften*, 2003).



- Kollmar, Frederike/El-Auwad, Maya*, Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, in: *Kommunikation und Recht* 2021, S. 73-78, (zit.: *Kollmar/El-Auwad*, K&R 2021, S. 73).
- Kramer, Ernst A.*, Juristische Methodenlehre, 6. Auflage, Bern 2019, (zit.: *Kramer*, Juristische Methodenlehre, 6. Aufl. 2019).
- Kramer, Stefan* [Hrsg.], IT-Arbeitsrecht, 3. Auflage, München 2023, (zit.: *Kramer/Bearbeiter*, IT-Arbeitsrecht, 3. Aufl. 2023).
- Krebs, Peter*, Die Begründungslast, in: *Archiv für die civilistische Praxis* 1995, Band 195, S. 171-211, (zit.: *Krebs*, AcP 195 (1995), S. 171).
- Kremer, Thomas/Bachmann, Gregor/Favoccia, Daniela/v. Werder, Axel* [Hrsg.], Deutscher Corporate Governance Kodex, 9. Auflage, München 2023, (zit.: *Kremer u.a./Bearbeiter*, DCGK, 9. Aufl. 2023).
- Krohm, Niclas*, Abschied vom Schriftformgebot der Einwilligung – Lösungsvorschläge und künftige Anforderungen, in: *Zeitschrift für Datenschutz* 2016, S. 368-373, (zit.: *Krohm*, ZD 2016, S. 368).
- Kroschwald, Steffen*, Verschlüsseltes Cloud Computing – Auswirkung der Kryptografie auf den Personenbezug in der Cloud, in: *Zeitschrift für Datenschutz* 2014, S. 75-80, (zit.: *Kroschwald*, ZD 2014, S. 75).
- Krügel, Tina*, Der Einsatz von Angriffserkennungssystemen im Unternehmen – Geeignete Maßnahmen zur Erhöhung der Informationssicherheit, in: *Zeitschrift für IT-Recht und Recht der Digitalisierung* 2017, S. 795-799, (zit.: *Krügel*, MMR 2017, S. 795).
- Krusche, Jan*, Kumulation von Rechtsgrundlagen zur Datenverarbeitung – Verhältnis der Einwilligung zu anderen Erlaubnistatbeständen, in: *Zeitschrift für Datenschutz* 2020, S. 232-237, (zit.: *Krusche*, ZD 2020, S. 232).
- Kühling, Jürgen*, Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung – Aufgabe des Rechts?, in: *Die Verwaltung* 2007, S. 155-172, (zit.: *Kühling*, *Die Verwaltung* 2007, S. 155).
- Kühling, Jürgen*, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen in: *Neue Juristische Wochenschrift* 2017, S. 1985-1990, (zit.: *Kühling*, *NJW* 2017, S. 1985).
- Kühling, Jürgen/Buchner, Benedikt* [Hrsg.], DS-GVO – BDSG, Kommentar, 4. Auflage, München 2024, (zit.: *Kühling/Buchner/Bearbeiter*, DS-GVO – BDSG, 4. Aufl. 2024).

*Kübling, Jürgen/Klar, Manuel/Sackmann, Florian*, Datenschutzrecht, 5. Auflage, Heidelberg 2021, (zit.: *Kübling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021).

*Kübling, Jürgen/Martini, Mario*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, in: Europäische Zeitschrift für Wirtschaftsrecht 2016, S. 448-454, (zit.: *Kübling/Martini*, EuZW 2016, S. 448).

*Kübling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/Nink, David/Weinzierl, Quirin/Wenzel, Michael*, Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016, (zit.: *Kübling* u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016).

*Kuner, Christopher/Bygrave, Lee A./Docksey, Christopher* [Hrsg.], The EU General Data Protection Regulation (GDPR), Kommentar, Oxford 2020, (zit.: *Kuner/Bygrave/Docksey/Bearbeiter*, GDPR, 2020).

*Küppers, Bastian*, Einführung in die Informatik, Wiesbaden 2022, (zit.: *Küppers*, Einführung in die Informatik, 2022).

*Küsters, Ralf/Wilke, Thomas*, Moderne Kryptographie, Wiesbaden 2011, (zit.: *Küsters/Wilke*, Moderne Kryptographie, 2011).

*Landmann/Rohmer*, Umweltrecht, Kommentar, Band I, Stand: 102. Ergänzungslieferung, München 2023, (zit.: *Landmann/Rohmer/Bearbeiter*, Umweltrecht, Bd. I, Stand: 102. EL. 2023).

*Langenbucher, Katja* [Hrsg.], Europäisches Privat- und Wirtschaftsrecht, 5. Auflage, Baden-Baden 2022, (zit.: *Langenbucher/Bearbeiter*, Europäisches Privat- und Wirtschaftsrecht, 5. Aufl. 2022).

*Larenz, Karl*, Methodenlehre der Rechtswissenschaft, 6. Auflage, Berlin u.a. 1991, (zit.: *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991).

*Laue, Philip*, Öffnungsklauseln in der DS-GVO – Öffnung wohin? – Geltungsbereich einzelstaatlicher (Sonder-)Regelungen, in: Zeitschrift für Datenschutz 2016, S. 463-467, (zit.: *Laue*, ZD 2016, S. 463).

*Laue, Philip/Kremer, Sascha*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage, Baden-Baden 2019, (zit.: *Laue/Kremer/Bearbeiter*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019).

*Leeb, Christina-Maria/Liebhaber, Johannes*, Grundlagen des Datenschutzrechts, in: Juristische Schulung 2018, S. 534-538, (zit.: *Leeb/Liebhaber*, JuS 2018, S. 534).

- Leisner, Walter Georg*, Die subjektiv-historische Auslegung des Gemeinschaftsrechts – Der "Wille des Gesetzgebers" in der Judikatur des EuGH, in: *Europarecht* 2007, S. 689-707, (zit.: *Leisner*, *EuR* 2007, S. 689).
- Leupold, Andreas/Wiebe, Andreas/Glossner, Silke* [Hrsg.], *IT-Recht*, 4. Auflage, München 2021, (zit.: *Leupold/Wiebe/Glossner/Bearbeiter*, *IT-Recht*, 4. Auflage 2021).
- v. Lewinski, Kai/Rüpkke, Giselher/Eckhardt, Jens*, *Datenschutzrecht*, 2. Auflage, München 2022, (zit.: *v. Lewinski/Rüpkke/Eckhardt*, *Datenschutzrecht*, 2. Aufl. 2022).
- Loewenheim, Ulrich/Meessen, Karl M./Riesenkampff, Alexander/Kersting, Christian/Meyer-Lindemann, Hans Jürgen* [Hrsg.], *Kartellrecht, Kommentar*, 4. Auflage, München 2020, (zit.: *Loewenheim u.a./Bearbeiter*, *Kartellrecht*, 4. Aufl. 2020).
- Lotz, Benjamin/Wendler, Julia*, Datensicherheit als datenschutzrechtliche Anforderung: Zur Frage der Abdingbarkeit des § 9 BDSG – Eine Erörterung für den privaten Rechtsverkehr und für Betreiber Kritischer Infrastrukturen, in: *Computer und Recht* 2016, S. 31-37, (zit.: *Lotz/Wendler*, *CR* 2016, S. 31).
- Lutter, Marcus*, Die Auslegung angeglichenen Rechts, in: *Juristen Zeitung* 1992, S. 593-607, (zit.: *Lutter*, *JZ* 1992, S. 593).
- Manssen, Gerrit*, *Staatsrecht II – Grundrechte*, 19. Auflage, München 2022, (zit.: *Manssen*, *Staatsrecht II*, 19. Aufl. 2022).
- Marschall, Kevin*, Datenpannen – „neue“ Meldepflicht nach der europäischen DS-GVO? – Rechtliche Änderungen durch Art. 31 und Art. 32 DS-GVO, in: *Datenschutz und Datensicherheit* 2015, S. 183-189, (zit.: *Marschall*, *DuD* 2015, S. 183).
- Martens, Sebastian A. E.*, *Methodenlehre des Unionsrechts*, Tübingen 2013, (zit.: *Martens*, *Methodenlehre des Unionsrechts*, 2013).
- Maslewski, Daniel*, Datenpannen-Management in der Unternehmenspraxis. Anforderungen der DS-GVO – Was gilt es bei einem Datenschutzvorfall zu beachten?, in: *Zeitschrift für Datenschutz* 2023, S. 251-256, (zit.: *Maslewski*, *ZD* 2023, S. 251).
- Matejek, Michael/Mäusezahl, Steffen*, Gewöhnliche vs. sensible personenbezogene Daten – Abgrenzung und Verarbeitungsrahmen von Daten gem. Art. 9 DS-GVO, in: *Zeitschrift für Datenschutz* 2019, S. 551-556, (zit. *Matejek/Mäusezahl*, *ZD* 2019, S. 551).
- Maurer, Hartmut/Waldhoff, Christian*, *Allgemeines Verwaltungsrecht*, 21. Auflage, München 2024, (zit.: *Maurer/Waldhoff*, *Allgemeines Verwaltungsrecht*, 21. Aufl. 2024).

- Mester, Britta Alexandra*, Informationelle Selbstbestimmung in Zeiten der Datenschutz-Grundverordnung – Datenschutz und Informationssicherheit im Lichte der Datenschutz-Grundverordnung, in: Sprech-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian/Thomsen, Oliver [Hrsg.]: Festschrift für Jürgen Taeger, S. 291-305, Frankfurt a.M. 2020, (zit.: *Mester*, Informationelle Selbstbestimmung in Zeiten der Datenschutz-Grundverordnung, in: FS Taeger, 2020, S. 291).
- Mestmäcker, Ernst-Joachim/Schweitzer, Heike*, Europäisches Wettbewerbsrecht, 3. Auflage, München 2014, (zit.: *Mestmäcker/Schweitzer*, Europäisches Wettbewerbsrecht, 3. Aufl. 2014).
- Meyer, Jürgen/Hölscheidt, Sven* [Hrsg.], Charta der Grundrechte der Europäischen Union, Kommentar, 5. Auflage, Baden-Baden 2019, (zit.: *Meyer/Hölscheidt/Bearbeiter*, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019).
- Meyer, Sebastian*, Bußgelder bei Datenschutzverstößen: Alles nur halb so schlimm?, in: Zeitschrift für Vertriebsrecht 2021, S. 1-3, (zit.: *Meyer*, ZVertriebsR 2021, S. 1).
- Michl, Walther*, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, in: Datenschutz und Datensicherheit 2017, S. 349-353, (zit.: *Michl*, DuD 2017, S. 349).
- Möllers, Thomas M.J.*, Juristische Methodenlehre, 5. Auflage, München 2023, (zit.: *Möllers*, Juristische Methodenlehre, 5. Aufl. 2023).
- Monreal, Manfred*, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO – Chancen nicht nur für das europäische Verständnis des Zweckbindungsgrundsatzes, in: Zeitschrift für Datenschutz 2016, S. 507-512, (zit.: *Monreal*, ZD 2016, S. 507).
- Moos, Flemming/Schefzig, Jens/Arning, Alexander* [Hrsg.], Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle, 2. Auflage, Frankfurt a.M. 2021, (zit.: *Moos/Schefzig/Arning/Bearbeiter*, Praxishandbuch DSGVO, 2. Aufl. 2021).
- Müller, Bernhard*, „Babylonische Sprachverwirrung“ – Methodologische Überlegungen zur Auslegung mehrsprachig verbindlicher Rechtstexte in der Europäischen Union, in: Jabloner, Clemens/Kucsko-Stadlmayer, Gabriele/Muzak, Gerhard/Perthold-Stoitzner, Bettina/Stöger, Karl [Hrsg.]: Vom praktischen Wert der Methode – Festschrift für Heinz Mayer, S. 391-411, Wien 2011, (zit.: *Müller*, „Babylonische Sprachverwirrung“, in: FS Mayer, 2011, S. 391).
- Müller, Friedrich/Christensen, Ralph*, Juristische Methodik, II. Band Europarecht, 3. Auflage, Berlin 2012, (zit.: *Müller/Christensen*, Juristische Methodik, II. Bd. Europarecht, 3. Aufl. 2012).

- Müller, Klaus-Rainer*, Handbuch Unternehmenssicherheit, 4. Auflage, Wiesbaden 2022, (zit.: *Müller*, Hdb. Unternehmenssicherheit, 4. Aufl. 2022),
- Münchener Kommentar zum Handelsgesetzbuch, Band 2, 5. Auflage, München 2022, (zit.: *MüKo HGB/Bearbeiter*, 5. Aufl. 2022).
- Münchener Kommentar zum Wettbewerbsrecht, 1. Band Europäisches Wettbewerbsrecht, 4. Auflage, München 2023, (zit.: *MüKo Wettbewerbsrecht/Bearbeiter*, Bd. 1, 4. Aufl. 2023).
- Paal, Boris P./Pauly, Daniel A.* [Hrsg.], Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Auflage, München 2021, (zit.: *Paal/Pauly/Bearbeiter*, DS-GVO BDSG, 3. Aufl. 2021).
- Paar, Christof/Pelzl, Jan*, Kryptografie verständlich, Berlin und Heidelberg 2016, (zit.: *Paar/Pelzl*, Kryptografie verständlich, 2016).
- Peifer, Markus*, Bessere Rechtssetzung als Leitbild europäischer Gesetzgebung, Berlin 2011, (zit.: *Peifer*, Bessere Rechtssetzung als Leitbild europäischer Gesetzgebung, 2011).
- Piltz, Carlo*, Die Datenschutz-Grundverordnung – Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Datenverarbeitung, in: Kommunikation und Recht 2016, S. 557-567, (zit.: *Piltz*, K&R 2016, S. 557).
- Piltz, Carlo*, Die Datenschutz-Grundverordnung – Teil 2: Rechte der Betroffenen und korrespondierende Pflichten des Verantwortlichen, in: Kommunikation und Recht 2016, S. 629-637, (zit.: *Piltz*, K&R 2016, S. 629).
- Piltz, Carlo*, Die Datenschutz-Grundverordnung – Teil 3: Rechte und Pflichten des Verantwortlichen und Auftragsverarbeiters, in: Kommunikation und Recht 2016, S. 709-717, (zit.: *Piltz*, K&R 2016, S. 709).
- Piltz, Carlo*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand – Wann dürfen personenbezogene Daten zum Zweck der Daten- und IT-Sicherheit verwendet werden?, in: Sprech-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian/Thomsen, Oliver [Hrsg.]: Festschrift für Jürgen Taeger, S. 351-359, Frankfurt a.M. 2020, (zit.: *Piltz*, „Sicherheit der Verarbeitung“ als gesetzlicher Erlaubnistatbestand, in: FS Taeger, 2020, S. 351).
- Plath, Kai-Uwe* [Hrsg.], DSGVO/BDSG/TTDSG, Kommentar, 4. Auflage, Köln 2023, (zit.: *Plath/Bearbeiter*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023).
- Poncza, Manuel*, Datenschutzrechtliche Grundlagen der sog. „Penetration Tests“ – Die Erlaubnistatbestände nach der DS-GVO, in: Zeitschrift für Datenschutz 2023, S. 8-13, (zit.: *Poncza*, ZD 2023, S. 8).

- Rebbahn, Robert*, Zur Methodenlehre des Unionsrechts – insbesondere im Privatrecht. Stefan Griller zum 60. Geburtstag gewidmet, in: Zeitschrift für die gesamte Privatrechtswissenschaft 2016, S. 281-306, (zit.: *Rebbahn*, ZfPW 2016, S. 281).
- Reimer, Franz*, Juristische Methodenlehre, 2. Auflage, Baden-Baden 2020, (zit.: *Reimer*, Juristische Methodenlehre, 2. Aufl. 2020).
- Richter, Philipp*, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, in: Datenschutz und Datensicherheit 2015, S. 735-740, (zit.: *Richter*, DuD 2015, S. 735).
- Riesenhuber, Karl* [Hrsg.], Europäische Methodenlehre, 4. Auflage, Berlin und Boston 2021, (zit.: *Riesenhuber/Bearbeiter*, Europäische Methodenlehre, 4. Aufl. 2021).
- Rippe, Klaus Peter*, Risiko, Ethik und die Frage des Zumutbaren, in: Zeitschrift für philosophische Forschung 2013, Band 67, S. 517-537, (zit.: *Rippe*, ZphF 67 (2013), S. 517).
- Ritter, Franziska/Reibach, Boris/Lee, Morris*, Lösungsvorschlag für eine praxisgerechte Risiko- beurteilung von Verarbeitungen – Ansatz zur Bestimmung von Eintrittswahrscheinlichkeit und Schadensausmaß bei der Bewertung datenschutzrechtlicher Risiken, in: Zeitschrift für Datenschutz 2019, S. 531-535, (zit.: *Ritter/Reibach/Lee*, ZD 2019, S. 531).
- Robrahn, Rasmus/Bremert, Benjamin*, Interessenskonflikte im Datenschutzrecht – Rechtferti- gung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO, in: Zeitschrift für Datenschutz 2018, S. 291-297, (zit.: *Robrahn/Bremert*, ZD 2018, S. 291).
- Roth, Wulf-Henning*, Europäische Verfassung und europäische Methodenlehre, in: Rabels Zeitschrift für ausländisches und internationales Privatrecht 2011, Band 75, S. 787-844, (zit.: *Roth*, RabelsZ 75 (2011), S. 787).
- Roßnagel, Alexander*, Wie zukunftsfähig ist die Datenschutz-Grundverordnung? Welche Ant- worten bietet sie für die neuen Herausforderungen des Datenschutzrecht?, in: Datenschutz und Datensicherheit 2016, S. 561-565, (zit.: *Roßnagel*, DuD 2016, S. 561).
- Roßnagel, Alexander* [Hrsg.], Das neue Datenschutzrecht, Baden-Baden 2018, (zit.: *Roßna- gel/Bearbeiter*, Das neue Datenschutzrecht, 2018).
- Roßnagel, Alexander*, Pseudonymisierung personenbezogener Daten – Ein zentrales Instru- ment im Datenschutz nach der DS-GVO, in: Zeitschrift für Datenschutz 2018, S. 243-247, (zit.: *Roßnagel*, ZD 2018, S. 243).

- Roßnagel, Alexander*, Kein „Verbotsprinzip“ und kein „Verbot mit Erlaubnisvorbehalt“ im Datenschutzrecht – Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff, in: Neue Juristische Wochenschrift 2019, S. 1-5, (zit.: *Roßnagel*, NJW 2019, S. 1).
- Roßnagel, Alexander/Müller, Jürgen*, Ubiquitous Computing – neue Herausforderungen für den Datenschutz. Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze, in: Computer und Recht 2004, S. 625-632, (zit.: *Roßnagel/Müller*, CR 2004, S. 625).
- Roßnagel, Alexander/Nebel, Maxi/Richter, Philipp*, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, in: Zeitschrift für Datenschutz 2015, 455-460, (zit.: *Roßnagel/Nebel/Richter*, ZD 2015, S. 455).
- Roßnagel, Alexander/Scholz, Philip*, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, in: Zeitschrift für IT-Recht und Recht der Digitalisierung 2000, S. 721-731, (zit.: *Roßnagel/Scholz*, MMR 2000, S. 721).
- Rüthers, Bernd/Fischer, Christian/Birk, Axel*, Rechtstheorie, 12. Auflage, München 2022, (zit.: *Rüthers/Fischer/Birk*, Rechtstheorie, 12. Aufl. 2022).
- Saeltzer, Gerhard*, Sind diese Daten personenbezogen oder nicht?, in: Datenschutz und Datensicherheit 2004, S. 218-227, (zit.: *Saeltzer*, DuD 2004, S. 218).
- Sander, Stefan*, Technische und organisatorische Maßnahmen im Rahmen der Auftragsverarbeitung gem. Art. 28 DSGVO, in: Privacy in Germany 2017, S. 250-256, (zit.: *Sander*, PinG 2017, S. 250).
- Sassenberg, Thomas/Faber, Tobias* [Hrsg.], Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Auflage, München 2020, (zit.: *Sassenberg/Faber/Bearbeiter*, Rechtshandbuch Industrie 4.0 und IoT, 2. Aufl. 2020).
- Schantz, Peter*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, in: Neue Juristische Wochenschrift 2016, S. 1841-1847, (zit.: *Schantz*, NJW 2016, S. 1841).
- Schantz, Peter/Wolff, Heinrich Amadeus*, Das neue Datenschutzrecht, München 2017, (zit.: *Schantz/Wolff/Bearbeiter*, Das neue Datenschutzrecht, 2017).
- Schild, Hans-Hermann*, Durchsetzung der DSGVO bei grenzüberschreitenden Datenschutzbeschwerden – Anmerkung zu dem vorgelegten Verordnungsentwurf der EU-Kommission, in: Datenschutz und Datensicherheit 2023, S. 565-570, (zit.: *Schild*, DuD 2023, S. 565).

- Schladebach, Marcus*, Praktische Konkordanz als verfassungsrechtliches Kollisionsprinzip – Eine Verteidigung, in: *Der Staat* 2014, Volumen 53, S. 263-283, (zit.: *Schladebach*, *Der Staat* Vol. 53 (2014), S. 263).
- Schläger, Uwe/Thode, Jan-Christoph* [Hrsg.], *Handbuch Datenschutz und IT-Sicherheit*, 2. Auflage, Berlin 2022, (zit.: *Schläger/Thode/Bearbeiter*, *Hdb. Datenschutz und IT-Sicherheit*, 2. Aufl. 2022).
- Schlegel, Hendrik*, Data-Loss-Prevention(DLP)-Software zur verdachtslosen Kontrolle ausgehender E-Mails – Datenschutzrechtliche Anforderungen und Grenzen der Verhältnismäßigkeit, in: *Zeitschrift für Datenschutz* 2020, S. 243-248, (zit.: *Schlegel*, *ZD* 2020, S. 243).
- Schleipfer, Stefan*, Pseudonymität in verschiedenen Ausprägungen – Wie gut ist die Unterstützung der DS-GVO, in: *Zeitschrift für Datenschutz* 2020, S. 284-291, (zit.: *Schleipfer*, *ZD* 2020, S. 284).
- Schmid, Carl*, Genehmigungsvorbehalt und Verbot mit Erlaubnisvorbehalt, in: *Die Öffentliche Verwaltung* 1954, S. 243-244, (zit.: *Schmid*, *DÖV* 1954, S. 243).
- Schmidt, Bernd/Roschek, Anna-Kristina*, Datenschutz im anwaltlichen Home- und Mobile-Office, in: *Neue Juristische Wochenschrift* 2021, S. 367-370, (zit.: *Schmidt/Roschek*, *NJW* 2021, S. 367).
- Schneider, Jana/Schindler, Stephan*, Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten – Datenschutzrechtliche Anforderungen beim Erheben von Videodaten, in: *Zeitschrift für Datenschutz* 2018, S. 463-469, (zit.: *Schneider/Schindler*, *ZD* 2018, S. 463).
- Schneider, Joben*, *Datenschutz*, 2. Auflage, München 2019, (zit.: *Schneider*, *Datenschutz*, 2. Aufl. 2019).
- Schoch, Friedrich*, Die Europäisierung des Allgemeinen Verwaltungsrechts, in: *Juristen Zeitung* 1995, S. 109-123, (zit.: *Schoch*, *JZ* 1995, S. 109).
- Schön, Wolfgang*, Die Analogie im Europäischen (Privat-)Recht, in: Auer, Marietta/Grigoleit, Hans Christoph/Hager, Johannes/Herresthal, Carsten/Hey, Felix/Koller, Ingo/Langenbacher, Katja/Neuner, Jörg/Petersen, Jens/Riehm, Thomas/Singer, Reinhard [Hrsg.]: *Festschrift für Claus-Wilhelm Canaris zum 80. Geburtstag*, S. 147-180, Berlin und Boston 2017, (zit.: *Schön*, *Die Analogie im Europäischen (Privat-)Recht*, in: *FS Canaris zum 80. Geburtstag*, 2017, S. 147).
- Schröder, Georg F.*, *Datenschutzrecht für die Praxis*, 5. Auflage, München 2023, (zit.: *Schröder*, *Datenschutzrecht für die Praxis*, 5. Aufl. 2023).



- Schröder, Markus*, Der risikobasierte Ansatz in der DS-GVO – Risiko oder Chance für den Datenschutz?, in: Zeitschrift für Datenschutz 2019, S. 503-506, (zit.: *Schröder*, ZD 2019, S. 503).
- Schulte, Laura/Wambach, Tim*, Zielkonflikte zwischen Datenschutz und IT-Sicherheit im Kontext der Aufklärung von Sicherheitsvorfällen, in: Datenschutz und Datensicherheit 2020, S. 462-468, (zit.: *Schulte/Wambach*, DuD 2020, S. 462).
- Schulze, Reiner* [Hrsg.], Bürgerliches Gesetzbuch, Kommentar, 11. Auflage, Baden-Baden 2022, (zit.: *Schulze/Bearbeiter*, BGB, 11. Aufl. 2022).
- Schulze, Reiner/Janssen, André/Kadelbach, Stefan* [Hrsg.], Europarecht, 4. Auflage, Baden-Baden 2020, (zit.: *Schulze/Janssen/Kadelbach/Bearbeiter*, Europarecht, 4. Aufl. 2020).
- Schünemann, Wolfgang B.*, Generalklausel und Regelbeispiele, in: Juristen Zeitung 2005, S. 271-279, (zit.: *Schünemann*, JZ 2005, S. 271).
- Schuster, Fabian/Grützmacher, Malte* [Hrsg.], IT-Recht, Kommentar, Köln 2020, (zit.: *Schuster/Grützmacher/Bearbeiter*, IT-Recht, 2020).
- Schwartzmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelman, Dieter* [Hrsg.], DS-GVO/BDSG Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 2. Auflage, Heidelberg 2020, (zit.: *Schwartzmann u.a./Bearbeiter*, DS-GVO/BDSG, 2. Aufl. 2020).
- Schwarze*, EU-Kommentar, 4. Auflage, Baden-Baden 2019, (zit.: *Schwarze/Knecht*, EU-Kommentar, 4. Aufl. 2019).
- Schweitzer, Heike*, Die Bedeutung nicht-wettbewerblicher Aspekte für die Auslegung von Art. 101 AEUV im Lichte der Querschnittsklauseln, in: Monopolkommission [Hrsg.]: Politischer Einfluss auf Wettbewerbsentscheidungen, S. 21-38, Baden-Baden 2015, (zit.: *Schweitzer*, Die Bedeutung nicht-wettbewerblicher Aspekte für die Auslegung von Art. 101 AEUV im Lichte der Querschnittsklauseln, in: Politischer Einfluss auf Wettbewerbsentscheidungen, 2015, S. 21).
- Seufert, Julia*, Datensicherheit in autonomen Fahrzeugen – Technische und organisatorische Maßnahmen für Fahrzeughersteller, in: Zeitschrift für Datenschutz 2023, S. 256-261, (zit.: *Seufert*, ZD 2023, S. 256).
- Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döbmann, Indra* [Hrsg.], Datenschutzrecht, Kommentar, Baden-Baden 2019, (zit.: *Simitis/Hornung/Spiecker gen. Döbmann/Bearbeiter*, Datenschutzrecht, 2019).

- Sosnitza, Olaf/Meisterernst, Andreas* [Hrsg.], Lebensmittelrecht, Stand: 186. Ergänzungslieferung, München 2023, (zit.: *Sosnitza/Meisterernst/Bearbeiter*, Lebensmittelrecht, Stand: 186. EL. 2023).
- Specht, Louisa/Mantz, Reto* [Hrsg.], Handbuch Europäisches und deutsches Datenschutzrecht, München 2019, (zit.: *Specht/Mantz/Bearbeiter*, Hdb. Europäisches und deutsches Datenschutzrecht, 2019).
- Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne* [Hrsg.], Datenrecht in der Digitalisierung, Berlin 2020, (zit.: *Specht-Riemenschneider/Werry/Werry/Bearbeiter*, Datenrecht in der Digitalisierung, 2020).
- Spiecker gen. Döhmman, Indra/Papakonstantinou, Vagelis/Hornung, Gerrit/De Hert, Paul* [Hrsg.], General Data Protection Regulation, Baden-Baden 2023, (zit.: *Spiecker gen. Döhmman u.a./Bearbeiter*, GDPR, 2023).
- Spies, Ulrich*, Zweckfestlegung der Datenverarbeitung durch den Verantwortlichen, in: Zeitschrift für Datenschutz 2022, S. 75-81, (zit.: *Spies*, ZD 2022, S. 75).
- Spindler, Gerald/Schuster, Fabian* [Hrsg.], Recht der elektronischen Medien, Kommentar, 4. Auflage, München 2019, (zit.: *Spindler/Schuster/Bearbeiter*, Recht der elektronischen Medien, 4. Aufl. 2019).
- Staatslexikon, Recht – Wirtschaft – Gesellschaft, 4. Band, Milieu – Schuldrecht, 8. Auflage, Freiburg im Breisgau 2020, (zit.: *Staatslexikon/Bearbeiter*, 4. Bd., 8. Aufl. 2020).
- Stern, Klaus/Sodan, Helge/Möstl, Markus* [Hrsg.], Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, Band III Allgemeine Lehren der Grundrechte, 2. Auflage, München 2022, (zit.: *Stern/Sodan/Möstl/Bearbeiter*, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III, 2. Aufl. 2022).
- Streinz, Rudolf* [Hrsg.], EUV/AEUV, Kommentar, 3. Auflage, München 2018, (zit.: *Streinz/Bearbeiter*, EUV/AEUV, 3. Aufl. 2018).
- Sundermann, Steffen*, Abdingbarkeit technischer oder organisatorischer Maßnahmen – Ist ein Verzicht auf Maßnahmen nach Art. 32 DSGVO möglich?, in: Datenschutz und Datensicherheit 2021, S. 594-597, (zit.: *Sundermann*, DuD 2021, S. 594).
- Suwelack, Felix*, Datenschutzrechtliche Vorgaben für Homeoffice und Remote Work - Nachhaltige und rechtssichere Umstellung – New Work. New Normal. New Problems?, in: Zeitschrift für Datenschutz 2020, S. 561-566, (zit.: *Suwelack*, ZD 2020, S. 561).

- Sydow, Gernot/Marsch, Nikolaus* [Hrsg.], Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, Kommentar, 3. Auflage, Baden-Baden 2022, (zit.: Sydow/Marsch/*Bearbeiter*, DS-GVO – BDSG, 3. Aufl. 2022).
- Taeger, Jürgen/Gabel, Detlev* [Hrsg.], DSGVO – BDSG – TTDSG, Kommentar, 4. Auflage, Frankfurt a.M. 2022, (zit.: Taeger/Gabel/*Bearbeiter*, DSGVO – BDSG – TTDSG, 4. Aufl. 2022).
- Taeger, Jürgen/Pohle, Jan* [Hrsg.], Computerrechts-Handbuch, Stand: 38. Ergänzungslieferung, München 2023, (zit.: Taeger/Pohle/*Bearbeiter*, Computerrechts-Hdb., Stand: 38. EL. 2023).
- Taeger, Jürgen/Schweda, Sebastian*, Die gemeinsam mit anderen Erklärungen erteilte Einwilligung – Kritische Auseinandersetzung mit dem Urteil des EuGH und den Schlussanträgen zur Rs. Planet49, in: Zeitschrift für Datenschutz 2020, S. 124-129, (zit.: *Taeger/Schweda*, ZD 2020, S. 124).
- Terbechte, Jörg Philipp*, Die ungeschriebenen Tatbestandsmerkmale des europäischen Wettbewerbsrechts, Baden-Baden 2004, (zit.: *Terbechte*, Die ungeschriebenen Tatbestandsmerkmale des europäischen Wettbewerbsrechts, 2004).
- Thüsing, Gregor* [Hrsg.], Beschäftigtendatenschutz und Compliance, 3. Auflage, München 2021, (zit.: Thüsing/*Bearbeiter*, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021).
- Tinnefeld, Marie-Theres/Conrad, Isabell*, Die selbstbestimmte Einwilligung im europäischen Recht – Voraussetzungen und Probleme, in: Zeitschrift für Datenschutz 2018, S. 391-398, (zit.: *Tinnefeld/Conrad*, ZD 2018, S. 391).
- Trstenjak, Verica/Beysen, Erwin*, Das Prinzip der Verhältnismäßigkeit in der Unionsrechtsordnung, in: Europarecht 2012, S. 265-285, (zit.: *Trstenjak/Beysen*, EuR 2012, S. 265).
- Uhl, Andreas*, Venen Biometrie – Stand der Technik, in: Datenschutz und Datensicherheit 2020, S. 16-22, (zit.: *Uhl*, DuD 2020, S. 16).
- Ulmer-Eilfort, Constanze/Obergfell, Inés* [Hrsg.], Verlagsrecht, Kommentar, 2. Auflage, München 2021, (zit.: Ulmer-Eilfort/Obergfell/*Bearbeiter*, Verlagsrecht, 2. Aufl. 2021).
- Veil, Winfried*, Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, in: Zeitschrift für Datenschutz 2018, S. 9-16, (zit.: *Veil*, ZD 2018, S. 9).

- Veil, Winfried*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider – Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, in: *Neue Zeitschrift für Verwaltungsrecht* 2018, S. 686-696, (zit.: *Veil*, NVwZ 2018, S. 686).
- Veil, Winfried*, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, in: *Neue Juristische Wochenschrift* 2018, S. 3337-3344, (zit.: *Veil*, NJW 2018, S. 3337).
- Wächter, Michael*, Datenschutz im Unternehmen, 6. Auflage, München 2021, (zit.: *Wächter*, Datenschutz im Unternehmen, 6. Aufl. 2021).
- Walter, Konrad*, Rechtsfortbildung durch den EuGH, Berlin 2009, (zit.: *Walter*, Rechtsfortbildung durch den EuGH, 2009).
- Wank, Rolf*, Juristische Methodenlehre, München 2020, (zit.: *Wank*, Juristische Methodenlehre, 2020).
- Weber, Klaus* [Hrsg.], Rechtswörterbuch, Stand: 31. Edition, München 2023, (zit.: *Weber/Bearbeiter*, Rechtswörterbuch, Stand: 31. Ed. 2023, Begriff:).
- Weidenhammer, Detlef/Gundlach, Rocco*, Wer kennt den „Stand der Technik“? – Umsetzungsempfehlungen für Energienetzbetreiber, in: *Datenschutz und Datensicherheit* 2018, S. 106-110, (zit.: *Weidenhammer/Gundlach*, DuD 2018, S. 106).
- Weiler, Frank*, Grammatikalische Auslegung des vielsprachigen Unionsrechts, in: *Zeitschrift für Europäisches Privatrecht* 2010, S. 861-880, (zit.: *Weiler*, ZEuP 2010, S. 861).
- Wendzel, Steffen*, IT-Sicherheit für TCP/IP- und IoT-Netzwerke, 2. Auflage, Wiesbaden 2021, (zit.: *Wendzel*, IT-Sicherheit für TCP/IP- und IoT-Netzwerke, 2021).
- Wennemann, Thomas*, TOM und die Datenschutz-Grundverordnung – Eine praktische Umsetzung von technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO, in: *Datenschutz und Datensicherheit* 2018, S. 174-177, (zit.: *Wennemann*, DuD 2018, S. 174).
- Weth, Stephan/Herberger, Maximilian/Wächter, Michael/Sorge, Christoph* [Hrsg.], Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Auflage, München 2019, (zit.: *Weth u.a./Bearbeiter*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019).
- Wybitul, Tim* [Hrsg.], Handbuch EU-Datenschutz-Grundverordnung, Frankfurt a.M. 2017, (zit.: *Wybitul/Bearbeiter*, Hdb. EU-Datenschutz-Grundverordnung, 2017).
- Wybitul, Tim*, Vermeidung von DS-GVO-Risiken nach Datenpannen und Cyberangriffen, in: *Neue Juristische Wochenschrift* 2020, S. 2577-2582, (zit.: *Wybitul*, NJW 2020, S. 2577).

- Ziegenhorn, Gero/von Heckel, Katharina*, Datenverarbeitung durch Private nach der europäischen Datenschutzreform – Auswirkungen der Datenschutz-Grundverordnung auf die materielle Rechtmäßigkeit der Verarbeitung personenbezogener Daten, in: *Neue Zeitschrift für Verwaltungsrecht* 2016, S. 1585-1591, (zit.: *Ziegenhorn/v. Heckel*, *NVwZ* 2016, S. 1585).
- Ziegenhorn, Gero/Schulz-Große, Stefanie*, Der Grundsatz der Zweckbindung – Anforderungen an die Erhebung und weitere Verarbeitung personenbezogener Daten, in: *Zeitschrift für Datenschutz* 2023, S. 581-587, (zit.: *Ziegenhorn/Schulz-Große*, *ZD* 2023, S. 581).
- Zimmer, Daniel*, Begrüßung und Einführung: Wettbewerb und Politik – eine Einführung in das Thema, in: *Monopolkommission [Hrsg.]: Politischer Einfluss auf Wettbewerbsentscheidungen*, S. 8-10, Baden-Baden 2015, (zit.: *Zimmer*, *Begrüßung und Einführung: Wettbewerb und Politik – eine Einführung in das Thema*, in: *Politischer Einfluss auf Wettbewerbsentscheidungen*, 2015, S. 8).
- Zippelius, Reinhold*, *Juristische Methodenlehre*, 12. Auflage, München 2021, herausgegeben und bearbeitet: *Würtenberger, Thomas*, (zit.: *Zippelius*, *Juristische Methodenlehre*, 12. Aufl. 2021).



## Sonstige Quellen

### *Materialien der Datenschutzaufsichtsbehörden:*

#### *Artikel-29-Datenschutzgruppe (Artikel-29-Gruppe):*

Artikel-29-Datenschutzgruppe, Opinion 03/2013 on purpose limitation, WP 203, angenommen am 02.04.2013, abrufbar unter: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf) (zuletzt abgerufen: 05.11.2023), (zit.: Artikel-29-Gruppe, WP 203).

Artikel-29-Datenschutzgruppe, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, angenommen am 09.04.2014, abrufbar unter: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf) (zuletzt abgerufen: 13.01.2024), (zit.: Artikel-29-Gruppe, WP 217).

#### *Europäische Datenschutzausschuss (EDSA):*

Europäischer Datenschutzausschuss, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, Version 2.0, angenommen am 08.10.2019, abrufbar unter: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_de\\_0.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf) (zuletzt abgerufen: 05.11.2023), (zit.: EDSA, Leitlinien 2/2019).

Europäischer Datenschutzausschuss, Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20.10.2020, abrufbar unter: [https://edpb.europa.eu/system/files/2021-04/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default\\_v2.0\\_de.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf) (zuletzt abgerufen am 12.10.2023), (zit.: EDSA, Leitlinien 4/2019).

Europäischer Datenschutzausschuss, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1, angenommen am 24.05.2023, abrufbar unter: [https://edpb.europa.eu/system/files/2023-06/edpb\\_guidelines\\_042022\\_calculationofadministrativefines\\_en.pdf](https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf) (zuletzt abgerufen: 25.10.2023), (zit.: EDSA, Leitlinien 04/2022).

*Nationale Aufsichtsbehörden:*

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) [Deutschland], Pressemitteilung 30/19, BfDI verhängt Geldbußen gegen Telekommunikationsdienstleister, vom 09.12.2019, abrufbar unter: [https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2019/30\\_BfDIverhängtGeldbuße1u1.html](https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2019/30_BfDIverhängtGeldbuße1u1.html) (zuletzt abgerufen: 15.07.2023), (zit.: BfDI, Pressemitteilung 30/19, 09.12.2019).

Datenschutzbehörde (DSB) [Österreich], Bescheid, DSB-D213.692/0001-DSB/2018, vom 16.11.2018, abrufbar unter: [https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT\\_20181116\\_DSB\\_D213\\_692\\_0001\\_DSB\\_2018\\_00/DSBT\\_20181116\\_DSB\\_D213\\_692\\_0001\\_DSB\\_2018\\_00.pdf](https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181116_DSB_D213_692_0001_DSB_2018_00/DSBT_20181116_DSB_D213_692_0001_DSB_2018_00.pdf) (zuletzt abgerufen: 10.01.2024), (zit.: DSB, DSB-D213.692/0001-DSB/2018).

Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) [Deutschland], Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, vom 26.04.2018, abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/kp/dsk\\_kpnr\\_18.pdf](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf) (zuletzt abgerufen: 10.12.2023), (zit.: DSK, Kurzpapier Nr. 18).

Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) [Deutschland], Das Standard-Datenschutzmodell (SDM), Eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele, Version 3.0., beschlossen am 24.11.2022, abrufbar unter: <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/> (zuletzt abgerufen: 11.01.2024), (zit.: DSK, Standard-Datenschutzmodell, Version 3.0).

Information Commissioner's Office (IOC) [Vereinigtes Königreich], Penalty Notice, Case ref: COM0783542 British Airways plc, vom 16.10.2020, abrufbar unter: <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> (zuletzt abgerufen: 15.07.2023), (zit.: IOC, Penalty Notice, Case ref: COM0783542 British Airways plc, 16.10.2020).

Information Commissioner's Office (IOC) [Vereinigtes Königreich], Penalty Notice, Case ref: COM0804337 Marriott International Inc, vom 30.10.2020, abrufbar unter: <https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf> (zuletzt abgerufen: 15.07.2023), (zit.: IOC, Penalty Notice, Case ref: COM0804337 Marriott International Inc, 30.10.2020).



*Materialien anderer Behörden und Organisationen:*

Bundesamt für Sicherheit in der Informationstechnik (BSI) [Deutschland], BSI-Standard 200-2, IT-Grundschutz-Methodik, Version 1.0 vom 15.11.2017, abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI\\_Standards/standard\\_200\\_2.html?nn=128640](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html?nn=128640) (zuletzt abgerufen: 13.01.2024), (zit.: BSI, BSI-Standard 200-2, IT-Grundschutz-Methodik).

Bundesamt für Sicherheit in der Informationstechnik (BSI) [Deutschland], Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, TR-02102-1, Version: 2023-01 vom 09.01.2023, abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?\\_\\_blob=publicationFile&v=9](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=9) (zuletzt abgerufen: 06.11.2023), (zit.: BSI, TR-02102-1).

Zentrum für sichere Informationstechnologie – Austria (A-SIT)/Bundeskanzleramt (BKA) [Österreich], Österreichisches Informationssicherheitshandbuch, Version 4.4.0 vom 06.11.2023, abrufbar unter: <https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitshandbuecher/Oesterreichisches-Informationssicherheitshandbuch-BKA-A-SIT.html> (zuletzt abgerufen: 13.01.2024), (zit.: A-SIT/BKA, österreichisches Informationssicherheitshandbuch, Version 4.4.0).

*Gesetzesmaterialien:**Gesetzesvorschriften:*

Berichtigung der Datenschutz-Grundverordnung, Berichtigung der 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), ABl. L 127, vom 23.05.2018, S. 2 ff., (zit.: Berichtigung der Datenschutz-Grundverordnung, ABl. EU L. 127, vom 23.05.2018, S. 2).

Datenschutz-Grundverordnung, 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), ABl. L 119 vom 4.5.2016, S. 1 ff.

Datenschutzrichtlinie, 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, ABl. L 281 vom 23.11.1995, S. 31 ff.

Grundrechte-Charta (GrCh), Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391 ff.

Verordnung Nr. 1, Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Wirtschaftsgemeinschaft, zuletzt geändert durch die Verordnung (EU) 517/2013 des Rates vom 13. Mai 2013 zur Anpassung einiger Verordnungen und Beschlüsse in den Bereichen freier Warenverkehr, Freizügigkeit, Gesellschaftsrecht, Wettbewerbspolitik, Landwirtschaft, Lebensmittelsicherheit, Tier und Pflanzengesundheit, Verkehrspolitik, Energie, Steuern, Statistik, transeuropäische Netze, Justiz und Grundrechte, Recht, Freiheit und Sicherheit, Umwelt, Zollunion, Außenbeziehungen, Außen-, Sicherheits- und Verteidigungspolitik und Organe aufgrund des Beitritts der Republik Kroatien, ABl. Nr. 017 vom 06.10.1958, S. 0358 f. (Verordnung Nr. 1), ABl. L 158 vom 10.06.2013, S. 1 ff. (Verordnung (EU) 517/2013), konsolidierte Fassung abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:01958R0001-20130701&qid=1703326083851> (zuletzt abgerufen: 23.12.2023).

*Gesetzesentwürfe und weitere gesetzesbezogene Materialien:*

Erläuterungen zur Charta der Grundrechte, ABl. EU C 303, vom 14.12.2007, S. 17 ff., (zit. Erläuterungen zur Charta der Grundrechte, ABl. EU C 303, vom 14.12.2007, S. 17).

Europäische Kommission, 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, vom 24.06.2020, COM(2020) 264 final, abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0264&from=EN> (zuletzt abgerufen: 12.10.2023), (zit.: Europäische Kommission, Erster Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung, COM(2020) 264 final, vom 24.06.2020).

Europäische Kommission, 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), vom 25.01.2012, KOM(2012) 11 endgültig, abrufbar unter: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF> (zuletzt abgerufen: 12.10.2023), (zit.: Europäische Kommission, Kommissionsentwurf der DS-GVO, KOM(2012) 11 endgültig, vom 25.01.2012; Verweise auf Artikel erfolgen unter dem Hinweis „DS-GVO E (Kommission)“).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, vom 04.07.2023, COM(2023) 348 final, abrufbar unter: <https://eur-lex.europa.eu/resource.html?uri=cellar:d02eb625-1a4d-11ee-806b->

01aa75ed71a1.0003.02/DOC\_1&format=PDF (zuletzt abgerufen: 12.10.2023), (zit.: Europäische Kommission, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, COM(2023) 348 final, vom 04.07.2023).

Europäisches Parlament, Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), P7\_TA(2014)0212, abrufbar unter: [https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212\\_DE.pdf?redirect](https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_DE.pdf?redirect) (zuletzt abgerufen: 12.10.2023), (zit.: Europäisches Parlament, Parlamentsentwurf der DS-GVO, P7\_TA(2014)0212, vom 12.03.2014).

Rat der Europäischen Union, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Revised version of Chapters I-IV, vom 06.05.2013, 8004/2/13 REV 2, abrufbar unter: <https://data.consilium.europa.eu/doc/document/ST-8004-2013-REV-2/en/pdf> (zuletzt abgerufen: 12.10.2023), (zit.: Rat der Europäischen Union, Ratsdokument 8004/2/13 REV 2, vom 06.05.2013).

Rat der Europäischen Union, 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) – Vorbereitung einer allgemeinen Ausrichtung, vom 11.06.2015, 9565/15, abrufbar unter: <https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf> (zuletzt abgerufen: 12.10.2023), (zit.: Rat der Europäischen Union, Ratsentwurf der DS-GVO, Ratsdokument 9565/15, vom 11.06.2015; Verweise auf Artikel erfolgen unter dem Hinweis „DS-GVO E (Rat)“).

### *Internetquellen:*

CMS Law.Tax, GDPR Enforcement Tracker, abrufbar unter: <https://www.enforcementtracker.com> (zuletzt abgerufen: 14.01.2024), (zit.: CMS Law.Tax, <https://www.enforcementtracker.com>).

DLA Piper, GDPR fines and data breach survey: January 2023, abrufbar unter: <https://www.dlapiper.com/en-ae/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023> (abgefragt: 18.08.2023), (zit.: DLA Piper, GDPR fines and data breach survey: January 2023).

Europäische Union, Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union

mitwirken, 2015, DOI 10.2880/836230, abrufbar unter: <https://op.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-de/format-PDF> (zuletzt abgerufen: 18.10.2023), (zit.: Europäische Union, Gemeinsamer Leitfaden für das Abfassung von Rechtstexten, 2015, DOI 10.2880/836230).

Europäische Union, Sprachen, abrufbar unter: [https://european-union.europa.eu/principles-countries-history/languages\\_de](https://european-union.europa.eu/principles-countries-history/languages_de) (zuletzt abgerufen: 23.12.2023), (zit.: Europäische Union, Sprachen, unter: [https://european-union.europa.eu/principles-countries-history/languages\\_de](https://european-union.europa.eu/principles-countries-history/languages_de)).

## Rechtsprechungsverzeichnis

### *Entscheidungen des Europäischen Gerichtshofs (EuGH):*

EuGH, Urteil v. 01.06.1961, Rs. C-15/60 (Simon/Gerichtshof), ECLI:EU:C:1961:11 = BeckRS 2004, 71721.

EuGH, Urteil v. 15.07.1964, Rs. C-6/64 (Costa/E.N.E.L.), ECLI:EU:C:1964:66 = BeckRS 1964, 105086.

EuGH, Urteil v. 9.07.1969, Rs. C-5/69 (Voelk/Vervaecke), ECLI:EU:C:1969:35 = BeckRS 2004, 73207.

EuGH, Urteil v. 12.11.1969, Rs. C-29/69 (Stauder/Stadt Ulm), ECLI:EU:C:1969:57 = BeckRS 2004, 72956.

EuGH, Urteil v. 12.12.1974, Rs. C-36/74 (Walrave und Koch/Association Union Cycliste Internationale u.a.), ECLI:EU:C:1974:140 = BeckRS 2004, 70975.

EuGH, Urteil v. 03.02.1976, Rs. C-59/75 (Manghera u.a.), ECLI:EU:C:1976:14 = BeckRS 2004, 73375.

EuGH, Urteil v. 08.04.1976, Rs. C-48/75 (Royer), ECLI:EU:C:1976:57 = BeckRS 2004, 73177.

EuGH, Urteil v. 27.10.1977, Rs. C-30/77 (Regina/Bouchereau), ECLI:EU:C:1977:172 = BeckRS 2004, 73063.

EuGH, Urteil v. 12.10.1978, Rs. C-13/78 (Eggers), ECLI:EU:C:1978:182 = BeckRS 2004, 71501.

EuGH, Urteil v. 29.11.1978, Rs. C- 83/78 (Redmond), ECLI:EU:C:1978:214 = BeckRS 2004, 73798.

EuGH, Urteil v. 19.06.1979, Rs. C-180/78 (Brouwer-Kaune), ECLI:EU:C:1979:156 = BeckRS 2004, 72048.

EuGH, Urteil v. 19.06.1980, verb. Rs. C-41/79, C-121/79, C-796/79 (Testa), ECLI:EU:C:1980:163 = BeckRS 2004, 71137.

- EuGH, Urteil v. 27.11.1980, Rs. C-81/79 (Sorasio-Allo u.a./Kommission), ECLI:EU:C:1980:270 = BeckRS 2004, 73763.
- EuGH, Urteil v. 06.10.1982, Rs. C-283/81 (C.I.L.F.I.T.), ECLI:EU:C:1982:335 = BeckRS 1982, 108239.
- EuGH, Urteil v. 12.12.1985, Rs. C-165/84 (Krohn/BALM), ECLI:EU:C:1985:507 = BeckRS 2004, 71892.
- EuGH, Urteil v. 19.04.1988, Rs. C-27/87 (Erau-Jacquery/La Hesbignonne), ECLI:EU:C:1988:183 = BeckRS 2004, 72822.
- EuGH, Urteil v. 04.10.1991, Rs. C-183/90 (Van Dalfsen u.a./Van Loon u.a.), ECLI:EU:C:1991:379 = BeckRS 2004, 74756.
- EuGH, Urteil v. 07.12.1995, Rs. C-449/93 (Rockfon/Specialarbejderforbundet i Danmark, agissant pour Søren Nielsen u.a.), ECLI:EU:C:1995:420 = NZA 1996, S. 471.
- EuGH, Urteil v. 24.10.1996, Rs. C-72/95 (Kraaijeveld u.a.), ECLI:EU:C:1996:404 = NVwZ 1997, S. 473.
- EuGH, Urteil v. 02.04.1998, Rs. C-296/95 (The Queen/Commissioners of Customs and Excise, ex parte EMU Tabac u.a.), ECLI:EU:C:1998:152 = EuZW 1998, S. 503.
- EuGH, Urteil v. 28.04.1998, Rs. C-306/96 (Javico/Yves Saint Laurent Parfums), ECLI:EU:C:1998:173 = EuZW 1998, S. 404.
- EuGH, Urteil v. 20.11.2001, Rs. C-268/99 (Jany u.a.), ECLI:EU:C:2001:616 = NVwZ 2002, S. 326.
- EuGH, Urteil v. 06.12.2005, verb. Rs. C-453/03, C-11/04, C-12/04, C-194/04 (ABNA u.a.), ECLI:EU:C:2005:741 = BeckRS 2005, 70934.
- EuGH, Urteil v. 23.11.2006, Rs. C-238/05 (ASNEF-EQUIFAX und Administración del Estado), ECLI:EU:C:2006:734 = BeckRS 2006, 70910.
- EuGH, Urteil v. 17.07.2008, Rs. C-66/08 (Kozłowski), ECLI:EU:C:2008:437 = NJW 2008, S. 3201.
- EuGH, Urteil v. 21.10.2008, verb. Rs. C-200/07, C-201/07 (Marra), ECLI:EU:C:2007:356 = EuZW 2009, S. 23.

- EuGH, Urteil v. 16.12.2008, Rs. C-210/06 (Cartesio), ECLI:EU:C:2008:723 = IStR 2009, S. 59.
- EuGH, Urteil v. 16.12.2008, Rs. C-524/06 (Huber), ECLI:EU:C:2008:724 = MMR 2009, S. 171.
- EuGH, Urteil v. 16.12.2008, Rs. C-73/07 (Satakunnan Markkinapörssi und Satamedia), ECLI:EU:C:2008:727 = EuZW 2009, S. 108.
- EuGH, Urteil v. 02.04.2009, Rs. C-260/07 (Pedro IV Servicios), ECLI:EU:C:2009:215 = EuZW 2009, S. 374.
- EuGH, Urteil v. 23.04.2009, Rs. C-533/07 (Falco Privatstiftung und Rabitsch), ECLI:EU:C:2009:257 = NJW 2009, S. 1865.
- EuGH, Urteil v. 19.11.2009, verb. Rs. C-402/07, C-432/07 (Sturgeon u.a.), ECLI:EU:C:2009:716 = NJW 2010, S. 43.
- EuGH, Urteil v. 20.05.2010, Rs. C-434/08 (Harms), ECLI:EU:C:2010:285 = BeckRS 2010, 90607.
- EuGH, Urteil v. 03.06.2010, Rs. C-569/08 (Internetportal und Marketing), ECLI:EU:C:2010:311 = MMR 2010, S. 538.
- EuGH, Urteil v. 08.06.2010, Rs. C-58/08 (Vodafone u.a.), ECLI:EU:C:2010:321 = MMR 2010, S. 561.
- EuGH, Urteil v. 28.10.2010, Rs. C-203/09 (Volvo Car Germany), ECLI:EU:C:2010:647 = NJW-RR 2011, S. 255.
- EuGH, Urteil v. 09.11.2010, verb. Rs. C-92/09, C-93/09 (Volker und Markus Schecke und Eifert), ECLI:EU:C:2010:662 = EuZW 2010, S. 939.
- EuGH, Urteil v. 04.10.2011, verb. Rs. C-403/08, C-429/08 (Football Association Premier League u.a.), ECLI:EU:C:2011:631 = ZUM 2011, S. 803.
- EuGH, Urteil v. 24.11.2011, verb. Rs. C-468/10, C-469/10 (ASNEF), ECLI:EU:C:2011:777 = EuZW 2012, S. 37.
- EuGH, Urteil v. 14.02.2012, Rs. C-17/10 (Toshiba Corporation e.a.), ECLI:EU:C:2012:72 = EuZW 2012, S. 223.

EuGH, Urteil v. 03.07.2012, Rs. C-128/11 (UsedSoft), ECLI:EU:C:2012:407 = ZUM 2012, S. 661.

EuGH, Urteil v. 13.12.2012, Rs. C-226/11 (Expedia), ECLI:EU:C:2012:795 = NZKart 2013, S. 111.

EuGH, Urteil v. 30.05.2013, Rs. C-488/11 (Asbeek Brusse und de Man Garabito), ECLI:EU:C:2013:341 = NJW 2013, S. 2579.

EuGH, Urteil v. 30.05.2013, Rs. C-342/12 (Worten), ECLI:EU:C:2013:355 = ZD 2013, S. 437.

EuGH, Urteil v. 17.10.2013, Rs. C-291/12 (Schwarz), ECLI:EU:C:2013:670 = ZD 2013, S. 608.

EuGH, Urteil v. 08.04.2014, verb. Rs. C-293/12, C-594/12 (Digital Rights Ireland und Seitlinger u.a.), ECLI:EU:C:2014:238 = EuZW 2014, S. 459.

EuGH, Urteil v. 07.04.2016, Rs. C-324/14 (Partner Apelski Dariusz), ECLI:EU:C:2016:214 = NZBau 2016, S. 373.

EuGH, Urteil v. 18.10.2016, Rs. C-135/15 (Nikiforidis), ECLI:EU:C:2016:774 = NJW 2017, S. 141.

EuGH, Urteil v. 08.11.2016, Rs. C-41/15 (Dowling u.a.), ECLI:EU:C:2016:836 = EuZW 2016, S. 955.

EuGH, Urteil v. 09.03.2017, Rs. C-398/15 (Manni), ECLI:EU:C:2017:197 = BeckRS 2017, 103300.

EuGH, Urteil v. 04.05.2017, Rs. C-13/16 (Rīgas satiksme), ECLI:EU:C:2017:336 = BeckRS 2017, 108615.

EuGH, Urteil v. 19.10.2017, Rs. C-582/14 (Breyer), ECLI:EU:C:2016:779 = NJW 2016, S. 3579.

EuGH, Urteil v. 20.12.2017, Rs. C-434/16 (Nowak), ECLI:EU:C:2017:994 = NJW 2018, S. 767.

EuGH, Urteil v. 05.07.2018, Rs. C-339/17 (Verein für lauterer Wettbewerb), ECLI:EU:C:2018:539 = GRUR 2018, S. 1061.

EuGH, Urteil v. 24.09.2019, Rs. C-507/17 (Google [Räumliche Reichweite der Auslistung]), ECLI:EU:C:2019:772 = NJW 2019, S. 3499.



- EuGH, Urteil v. 03.10.2019, Rs. C-70/18 (A u.a.), ECLI:EU:C:2019:823 = BeckRS 2019, 23122.
- EuGH, Urteil v. 21.11.2019, Rs. C-678/18 (Procureur-Generaal bij de Hoge Raad der Nederlanden), ECLI:EU:C:2019:998 = GRUR 2020, S. 108.
- EuGH, Urteil v. 11.12.2019, Rs. C-708/18 (Asociația de Proprietari bloc M5A-ScaraA), ECLI:EU:C:2019:1064 = ZD 2020, S. 148.
- EuGH, Urteil v. 19.12.2019, Rs. C-263/18 (Nederlands Uitgeversverbond und Groep Algemene Uitgevers), ECLI:EU:C:2019:1111 = GRUR 2020, S. 179.
- EuGH, Urteil v. 18.06.2020, Rs. C-754/18 (Ryanair Designated Activity Company), ECLI:EU:C:2020:478 = BeckRS 2020, 12792.
- EuGH, Urteil v. 16.07.2020, Rs. C-311/18 (Facebook Ireland und Schrems), ECLI:EU:C:2020:559 = GRUR-RS 2020, 16082.
- EuGH, Urteil v. 10.12.2020, Rs. C-620/19 (J & S Service), ECLI:EU:C:2020:1011 = ZD 2021, S. 319.
- EuGH, Urteil v. 15.06.2021, Rs. C-645/19 (Facebook Ireland u.a.), ECLI:EU:C:2021:483 = NJW 2021, S. 2495.
- EuGH, Urteil v. 22.06.2021, Rs. C-439/19 (Latvijas Republikas Saeima ([Points de pénalité])), ECLI:EU:C:2021:504 = BeckRS 2021, 15289.
- EuGH, Urteil v. 02.09.2021, Rs. C-337/20 (CRCAM), ECLI:EU:C:2021:671 = BeckRS 2021, 24493.
- EuGH, Urteil v. 13.10.2022, verb. Rs. C-164/21, C-318/21 (BALTIJAS STARPTAUTISKĀ AKADĒMIJA), ECLI:EU:C:2022:785 = BeckRS 2022, 27275.
- EuGH, Urteil v. 08.12.2022, Rs. C-180/21 (Inspektor v Inspektorata kam Visshia sadeben savet [Finalités du traitement de données - Enquête pénale]), ECLI:EU:C:2022:967 = BeckRS 2022, 34896.
- EuGH, Urteil v. 20.04.2023, Rs. C-580/21 (EEW Energy from Waste), ECLI:EU:C:2023:304 = BeckRS 2023, 7670.
- EuGH, Urteil v. 27.04.2023, Rs. C-352/21 (A1 und A2 [Assurance d'un bateau de plaisance]), ECLI:EU:C:2023:344 = RdTW 2023, S. 345.

EuGH, Urteil v. 22.06.2023, Rs. C-579/21 (Pankki S), ECLI:EU:C:2023:501 = NZA 2023, S. 889.

EuGH, Urteil v. 03.07.2023, Rs. C-252/21 (Meta Platforms u.a. [Conditions générales d'utilisation d'un réseau social]), ECLI:EU:C:2023:537 = GRUR 2023, S. 1131.

EuGH, Urteil v. 14.12.2023, Rs. C-340/21 (Natsionalna agentsia za prihodite), ECLI:EU:C:2023:986 = BeckRS 2023, 35786.

EuGH, Urteil v. 21.12.2023, Rs. C-667/21 (Krankenversicherung Nordrhein), ECLI:EU:C:2023:1022 = BeckRS 2023, 36822.

*Schlussanträge der Generalanwälte des Europäischen Gerichtshofs (EuGH):*

GA Bobek, Schlussanträge v. 22.06.2016 zur Rs. C-177/15 (Nelsons), ECLI:EU:C:2016:474.

GA Bot, Schlussanträge v. 08.09.2016 zur Rs. C-398/15 (Manni), ECLI:EU:C:2016:652 = BeckRS 2016, 82240.

GA Jacobs, Schlussanträge v. 28.01.1999 zur Rs. C-67/96 (Albany), ECLI:EU:C:1999:28.

GA Kokott, Schlussanträge v. 08.05.2008 zur Rs. C-73/07 (Satakunnan Markkinapörssi und Satamedia), ECLI:EU:C:2008:266.

GA Kokott, Schlussanträge v. 01.03.2018 zur verb. Rs. C-118/16, C-115/16, C-118/16, C-119/16, C-299/16 (X Danemark), ECLI:EU:C:2018:146.

GA Medina, Schlussanträge v. 29.06.2023 zur verb. Rs. C-207/22, C-267/22, C-290/22 (Lineas – Concessões de Transportes), ECLI:EU:C:2023:533.

GA Trstenjak, Schlussanträge v. 14.05.2009 zur Rs. C-199/08 (Eschig), ECLI:EU:C:2009:310.

*Entscheidungen des Bundesverfassungsgerichts (BVerfG):*

BVerfG, Beschluss v. 26.05.1970, Az. 1 BvR 83/69, 1 BvR 244/69 und 1 BvR 345/69, BVerfGE 28, S. 243.

BVerfG, Beschluss v. 08.08.1978, Az. 2 BvL 8/77, BVerfGE 49, S. 89.

BVerfG, Beschluss v. 27.01.1998, Az. 1 BvL 15/87, ECLI:DE:BVerfG:1998:ls19980127.1bvl001587 = BVerfGE 97, S. 169.

BVerfG, Beschluss v. 23.10.2013, Az. 1 BvR 1842/11 und 1 BvR 1843/11,  
ECLI:DE:BVerfG:2013:rs20131023.1bvr184211 = BVerfGE 134, S. 204.

BVerfG, Beschluss v. 11.04.2018, Az. 1 BvR 3080/09,  
ECLI:DE:BVerfG:2018:rs20180411.1bvr308009 = BVerfGE 148, S. 267.

BVerfG, Beschluss v. 03.06.2022, Az. 1 BvR 2103/16,  
ECLI:DE:BVerfG:2022:rk20220603.1bvr210316 = NJW 2022, 2677.

*Entscheidungen der Zivilgerichte:*

RG (VI. Zivilsenat), Urteil v. 29.04.1904, Rep. VI. 311/03 = RGZ 57, S. 353.

BGH (I. Zivilsenat), Urteil v. 18.01.2012, Az. I ZR 187/10 = BGHZ 192, S. 204.

LG Bonn, Urteil v. 11.11.2020, Az. 29 OWi 1/20 = BeckRS 2020, 35663.

*Entscheidungen der Verwaltungsgerichte:*

VG Mainz, Urteil v. 20.02.2020, Az. 1 K 467/19.MZ = BeckRS 2020, 5397.

VG Mainz, Urteil v. 17.12.2020, Az. 1 K 778/19.MZ = CR 2021, S. 471.

*Entscheidungen der Sozialgerichte:*

LSG Hessen, Beschluss v. 29.01.2020, Az. L 4 SO 154/19 B = BeckRS 2020, 1442.