Datenschutzrecht: DatSchR

13. Auflage 2021
ISBN 978-3-406-77024-1
Beck im dtv

Datenschutzrecht

dtv

Schnellübersicht

Abgabenordnung (AO) (Auszug) 36
Artikel 10-Gesetz (G 10) 16
Betriebsverfassungsgesetz (BetrVG) (Auszug) 22
Bundesbeamtengesetz (BBG) (Auszug) 21
Bundesdatenschutzgesetz (BDSG) 6
Datenschutz-Grundverordnung (VO (EU) 2016/678) 1
Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) 3
Europäische Datenschutzkonvention (Konvention Nr. 108 des Europarats) 5
Fluggastdatengesetz (FlugDaG) 17
Geschäftsgeheimnis-Schutzgesetz (GeschGehG) (Auszug) 12
Grundgesetz (GG) (Auszug) 15
Grundrechtecharta (GRCh) 4
Handelsgesetzbuch (HGB) (Auszug) 35
Informationsfreiheitsgesetz (IFG) 7
JI-Richtlinie (RL (EU) 2016/680) 2
Kunsturhebergesetz (KUG) (Auszug) 13
Sozialgesetzbuch
– Allgemeiner Teil (SGB I) (Auszug) 23
– Grundsicherung für Arbeitsuchende (SGB II) (Auszug) 24
– Arbeitsförderung (SGB III) (Auszug) 25
– Sozialversicherung (SGB IV) (Auszug) 26
– Gesetzliche Krankenversicherung (SGB V) (Auszug) 27
– Gesetzliche Rentenversicherung (SGB VI) (Auszug) 28
– Gesetzliche Unfallversicherung (SGB VII) (Auszug) 29
– Kinder- und Jugendhilfe (SGB VIII) (Auszug) 30
– Rehabilitation und Teilhabe behinderter Menschen (SGB IX) (Auszug) 31
– Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X) (Auszug) 32
– Soziale Pflegeversicherung (SGB XI) (Auszug) 33
– Sozialhilfe (SGB XII) (Auszug) 34
Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46 EG 37–39
Strafgesetzbuch (StGB) (Auszug) 20
Strafprozessordnung (StPO) (Auszug) 19
Telekommunikationsgesetz (TKG) (Auszug) 9
Telekommunikations-Überwachungsverordnung (TKÜV) 10
Telemediengesetz (TMG) 8
Unlauterer Wettbewerb-Gesetz (UWG) (Auszug) 11
Unterlassungsklagengesetz (UKlaG) (Auszug) 14
Verwaltungsverfahrensgesetz (VwVfG) (Auszug) 18

Datenschutzrecht

Datenschutz-Grundverordnung
JI-Richtlinie
Bundesdatenschutzgesetz
Informationsfreiheitsgesetz
Grundrechtecharta · Grundgesetz (Auszug)
Europäische Datenschutzkonvention
Strafprozessordnung (Auszug) · Strafgesetzbuch (Auszug)
Telemediengesetz · Telekommunikationsgesetz (Auszug)
Fluggastdatengesetz
Bundesbeamtengesetz (Auszug)
Betriebsverfassungsgesetz (Auszug)
Standardvertragsklauseln für die Übermittlung
personenbezogener Daten in Drittländer

Textausgabe mit ausführlichem Sachverzeichnis
und einer Einführung von

Prof. Dr. Marcus Helfrich, Rechtsanwalt, München

13. Auflage
Stand: 15. April 2021

dtv

www.dtv.de
www.beck.de

Sonderausgabe
dtv Verlagsgesellschaft mbH & Co. KG,
Tumblingerstraße 21, 80337 München

Gesamtherstellung: Druckerei C.H. Beck, Nördlingen
(Adresse der Druckerei: Wilhelmstraße 9, 80801 München)
Umschlaggestaltung auf der Grundlage
der Gestaltung von Celestino Piatti

CO_2 neutral
chbeck.de/nachhaltig

ISBN 978-3-423-53085-9 (dtv)
ISBN 978-3-406-77024-1 (C.H. Beck)

Inhaltsverzeichnis

Abkürzungsverzeichnis IX
Einführung XIII

Erster Teil. Europäische Regelungen

1. 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) 1
2. Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie) 131
3. Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) 196
4. Charta der Grundrechte der Europäischen Union 219
5. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108 des Europarats) 253

Zweiter Teil. Nationales Recht

6. Bundesdatenschutzgesetz (BDSG) 263
7. Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz – IFG) 319
8. Telemediengesetz (TMG) 324
9. Telekommunikationsgesetz (TKG) (Auszug) 353
10. Telekommunikations-Überwachungsverordnung (TKÜV) 402
11. Gesetz gegen den unlauteren Wettbewerb (UWG) (Auszug) 430
12. Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) 432
13. Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz – KUG) (Auszug) 441
14. Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz – UKlaG) (Auszug) 442
15. Grundgesetz (GG) (Auszug) 446

Inhalt

16. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) 448
17. Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) 464
18. Verwaltungsverfahrensgesetz (VwVfG) (Auszug) 476
19. Strafprozeßordnung (StPO) (Auszug) 481
20. Strafgesetzbuch (StGB) (Auszug) 525
21. Bundesbeamtengesetz (BBG) (Auszug) 534
22. Betriebsverfassungsgesetz (BetrVG) (Auszug) 541
23. Sozialgesetzbuch (SGB) Erstes Buch – Allgemeiner Teil (SGB I) (Auszug) 551
24. Sozialgesetzbuch (SGB) Zweites Buch – Grundsicherung für Arbeitsuchende (SGB II) (Auszug) 557
25. Sozialgesetzbuch (SGB) Drittes Buch – Arbeitsförderung (SGB III) (Auszug) 563
26. Viertes Buch Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung – (SGB IV) (Auszug) 569
27. Sozialgesetzbuch (SGB) Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) (Auszug) 580
28. Sozialgesetzbuch (SGB) Sechstes Buch – Gesetzliche Rentenversicherung (SGB VI) (Auszug) 707
29. Siebtes Buch Sozialgesetzbuch – Gesetzliche Unfallversicherung (SGB VII) (Auszug) 719
30. Sozialgesetzbuch (SGB) Achtes Buch – Kinder- und Jugendhilfe (SGB VIII) (Auszug) 727
31. Sozialgesetzbuch (SGB) Neuntes Buch – Rehabilitation und Teilhabe von Menschen mit Behinderung (SGB IX) (Auszug) 731
32. Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) (Auszug) 732
33. Sozialgesetzbuch (SGB) Elftes Buch – Soziale Pflegeversicherung (SGB XI) (Auszug) 759
34. Sozialgesetzbuch (SGB) Zwölftes Buch – Sozialhilfe (SGB XII) (Auszug) 767
35. Handelsgesetzbuch (HGB) (Auszug) 771
36. Abgabenordnung (AO) (Auszug) 772

Dritter Teil. Materialien und Empfehlungen für die Praxis

37. Standardvertrag I. Standardvertragsklauseln im Sinne von Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten in Drittländer, die kein angemessenes Schutzniveau gewährleisten 775
38. Standardvertrag II. Standardvertragsklauseln für die Übermittlung personenbezogener Daten aus der Gemeinschaft in Drittländer 785

39. Standardvertragsklauseln (Auftragsverarbeiter). Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG 792

Sachverzeichnis 803

Inhalt

Einführung

von Prof. Dr. Marcus Helfrich, Rechtsanwalt, München

In der Netzgesellschaft hinterlassen wir Datenspuren. Betreiber sozialer Netzwerke bündeln die Einträge eines Mitglieds zu einem multimedialen Lebenslauf, Lieferanten entwickeln durch Empfehlungsalgorithmen Nutzerprofile ihrer Kunden, Marketingkonzepte stellen auf datenbasierte Verhaltensprognosen ab, in der Arbeitswelt bilden Unternehmen durch Monitoring-Systeme Kommunikationsmuster ihrer Mitarbeiter ab oder streben nach einer Optimierung von Geschäftsprozessen durch eine möglichst lückenlose Protokollierung des Arbeitsverhaltens. Schließlich wird allenthalben eine verheißungsvolle Zukunft mit Smart Home, autonomem Fahren oder auch der künftigen Produktion von Gütern im Rahmen der Industrie 4.0 gezeichnet. Staatliche Stellen sammeln Daten für die Strafverfolgung und ringen im Bemühen um die effektive Prävention terroristischer Bedrohungen sowie der wirksamen Verfolgung nationaler oder internationaler Kriminalität um die hierzu nötigen Informationen. Pandemische Gefährdungslagen lassen das Bedürfnis nach einer umfassenden Verarbeitung von Gesundheitsdaten sichtbar werden. In dieser vernetzten digitalen Gesellschaft hat das Datenschutzrecht die Aufgabe, das Recht auf informationelle Selbstbestimmung zu schützen und zugleich einen wirksamen Ausgleich zwischen miteinander streitenden Interessen und anderen grundrechtlich geschützten Positionen zu schaffen. Datenschutzrecht ist ein komplexes Recht, das ursprünglich aus dem nationalen Verfassungsrecht abgeleitet wurde und inzwischen durch die Datenschutz-Grundverordnung (DS-GVO) auf einer europaweit harmonisierten Grundlage beruht. Stand im Zuge der EG-Datenschutzrichtlinie des Jahres 1995 noch das Bemühen im Vordergrund, unter Beachtung des Subsidiaritätsprinzips auf nationaler Ebene ein möglichst harmonisiertes Datenschutzniveau zu schaffen, stiftet die Datenschutz-Grundverordnung mit ihrer Wirksamkeit seit dem 25. Mai 2018 ein einheitliches Datenschutzrecht[1] innerhalb der gesamten Europäischen Union (I.). In der Zukunft wird der Datenschutz in der wachsenden Netzgesellschaft mit mobiler Kommunikation, der Cloud gespeicherten Daten sowie dem „Internet der Dinge“ (IoT) seine Aufgabe und Wirkung finden müssen (VI.).

I. Datenschutz zwischen Europarecht und nationalem Recht

Die Verarbeitung personenbezogener Daten bildet eine der wesentlichen Säulen der Informationsgesellschaft und der in ihr erfolgreichen digitalen Wirtschaft. IT-Verarbeitungen sind nicht mehr nur lokal vorstellbar. Von der Erhebung personenbezogener Daten bis hin zur Verarbeitung und deren Speicherung in transnationalen oder internationalen Cloud-Lösungen finden IT-Prozesse im grenzüberschreitenden Kontext statt. Gleichzeitig bildet das jeweilige nationale Recht stets den Anknüpfungspunkt für die datenschutzrechtliche Ausgestaltung der IT-Prozesse. Der Europarat erkannte 1981 die grundrechtli-

[1] Siehe Erwägungsgrund 3 DS-GVO.

che Bedeutung des Schutzes des Persönlichkeitsrechts für den Einzelnen und verankerte im „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108)“ (**Nr. 5**) eine Verpflichtung der Unterzeichnerstaaten zu Schutz des Persönlichkeitsrechts im Zusammenhang mit der Verarbeitung personenbezogener Daten. Die Konvention stellt einen wichtigen Baustein der europäischen Datenschutzhistorie dar. Am 18. Mai 2018 legte das Ministerkomitee des Europarats eine modernisierte Fassung der Konvention vor („Konvention 108+“),[1] die jedoch bislang für die Bundesrepublik Deutschland noch nicht in Kraft getreten ist. Vom Abdruck in der vorliegenden Textsammlung wird deshalb einstweilen abgesehen.

Auf der Ebene der Europäischen Gemeinschaft verfolgte die EG-Datenschutzrichtlinie (RL 95/46/EG)[2] des Jahres 1995 das Ziel, die in den Mitgliedstaaten bestehende Rechtslage in Bezug auf den Schutz der personenbezogenen Daten zu harmonisieren und so innerhalb der Europäischen Gemeinschaft ein gemeinsames Datenschutzniveau zu bilden. Die Richtlinie wurde in den Mitgliedstaaten der EG umgesetzt. Allerdings führte dies nicht zu der angestrebten einheitlichen Handhabung des Datenschutzes. So waren die festzustellenden Unterschiede beim Schutz der Rechte und Grundfreiheiten von Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten für die Kommission Anlass, im Januar 2012 den Entwurf einer Datenschutz-Grundverordnung[3] dem ordentlichen Gesetzgebungsverfahren nach Art. 294 AEUV zuzuführen. Nach intensiven und teilweise langwierigen Beratungen und Verhandlungen, sowohl im Rahmen des Europaparlaments als auch des Rates der Europäischen Union, verständigten sich die im Gesetzgebungsverfahren beteiligten Organe im Rahmen des sog. „Trilogs“ am 15. Dezember 2015 auf eine gemeinsame Entwurfsfassung der Datenschutz-Grundverordnung (DS-GVO). Diese wurde am 27. April 2016 verabschiedet und am 4. Mai 2016 im Amtsblatt der EU veröffentlicht **(Nr. 1)**.[4] Zeitgleich wurde im Rahmen des verabschiedeten Datenschutzpakets die Richtlinie (EU) 2016/680 **(Nr. 2)** verabschiedet und veröffentlicht, mit der vor allen Dingen die datenschutzrechtlichen Rahmenbedingungen für die Strafverfolgung und -vollstreckung innerhalb der EU-Mitgliedstaaten harmonisiert werden sollen.[5]

Die DS-GVO ist seit dem 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union einheitlich zu beachten. Zeitgleich trat in der Bundesrepublik Deutschland ein grundlegend reformiertes Bundesdatenschutzgesetz (BDSG) **(Nr. 6)** in Kraft, mit dem der nationale Gesetzgeber sich um die Ausgestaltung

---

[1] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final v. 18.5.2018.

[2] RL 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. EG L 281, S. 31.

[3] Entwurf einer Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM/2012/011 endg. v. 25.1.2012.

[4] 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. EU L 119, S. 1 v. 4.5.2016.

[5] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU L 119, S. 89 v. 4.5.2016.

verbliebener oder eingeräumter datenschutzrechtlicher Regelungskompetenzen bemüht.

Als „Grundverordnung“[1] sieht die DS-GVO zwar einerseits allgemeine und grundlegende Regeln zur Verarbeitung[2] personenbezogener Daten vor. Andererseits enthält die Verordnung eine Vielzahl an Klauseln,[3] die den Mitgliedstaaten gestatten, ergänzende bzw. spezifischere Vorschriften des Schutzes personenbezogener Daten entweder aufrecht zu erhalten oder zu schaffen. Wie *Selmayr*[4] zutreffend betont, handelt es sich bei diesen Regelungen streng genommen nicht um „Öffnungsklauseln“, sondern um Spezifizierungsklauseln, da dem nationalen Gesetzgeber nur in dem durch die Verordnung vorgegebenen Rahmen der Erlass spezifizierender Vorschriften gestattet ist.

Der Bundesgesetzgeber sah sich in der Pflicht, über die unionsrechtlich geforderte Umsetzung der Richtlinie (EU) 2016/680 **(Nr. 2)** hinaus auch von der aus seiner Sicht eingeräumten rechtsgestaltenden Befugnis aufgrund zahlreicher als „Öffnungsklauseln“ wahrgenommenen Regelungen der DS-GVO Gebrauch zu machen. Dies geschah trotz erheblicher europarechtlicher Bedenken[5] mit der Verabschiedung des (Ersten) Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU). Das in dem Artikelgesetz enthaltene BDSG ist als **Nr. 6** in diesen Textband aufgenommen.

Mit dem „Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU)“[6] vom 20. November 2019 hat der Bundesgesetzgeber in mehr als 150 Einzelgesetzen überwiegend[7] redaktionelle Anpassungen vorgenommen. Im Rahmen dieses Gesetzgebungsvorhabens wurde die in § 38 Abs. 1 BDSG zuvor enthaltene Schwelle für die Benennung eines Datenschutzbeauftragten von zehn auf zwanzig Mitarbeiter angehoben.[8]

In welchem Umfang die Bestimmungen des BDSG neben der DS-GVO europarechtlich Bestand haben werden, bleibt ausdrücklich abzuwarten.[9] Die im Gesetzgebungsverfahren zum 1. DSAnpUG-EU geäußerte Kritik verweist sowohl darauf, dass der Bundesgesetzgeber teilweise in Verkennung der Bedeutung der Spezifizierungsklauseln über den Regelungsrahmen der DS-GVO hinausgeht als auch in anderer Hinsicht unter Verletzung des unionsrechtlichen Verbotes den Wortlaut und Regelungsgehalt der Verordnung im nationalen Recht wiederholt.

In jedem Fall bedürfen auch die bestehenden nationalen Datenschutzvorschriften vor dem Hintergrund des höherrangigen Europarechts jedenfalls der europarechtsfreundlichen Auslegung.[10]

---

[1] Zum Begriff der „Grundverordnung“ *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 82.

[2] Zum umfassenden Begriff der „Verarbeitung“ vgl. Art. 4 Nr. 2 DS-GVO.

[3] Vgl. beispielsweise Art. 6 Abs. 2 DS-GVO oder auch Art. 88 Abs. 1 DS-GVO.

[4] Vgl. *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 82 ff.

[5] *Jensen*, ZD-Aktuell 2017, 05596; *Ehmann*, ZD-Aktuell 2016, 04216; *Johannes*, ZD-Aktuell 2016, 05322; *Helfrich*, ZD 2017, 97; *Franck*, ZD 2018, 345.

[6] BGBl. I 1626 vom 25.11.2019.

[7] Zu den einzelnen Änderungen und deren Begründung vgl. BR-Drs. 430/18 vom 7.9.2018 S. 2 ff.

[8] Hierzu *Helfrich* in: Sydow, Bundesdatenschutzgesetz, 2020, § 38 Rn. 40.

[9] Siehe hierzu *Franck*, ZD 2018, 345.

[10] Die vorliegende Textsammlung nimmt auf diese Parallelität der datenschutzrechtlichen Regelungsebenen insoweit Rücksicht, als der DS-GVO wegen ihres Vorrangs in der Gliederungssystematik

Einführung

Die DS-GVO bringt einen teilweise erheblichen Änderungs- oder Anpassungsbedarf mit sich: Die für die Verarbeitung verantwortlichen müssen ihre Verfahren und Abläufe so gestalten, dass eine möglichst hohe Datenschutzfreundlichkeit gewährleistet ist („Privacy by Design" sowie „Privacy by Default"),[1] dem Betroffenen werden unter dem Schlagwort des „Rechts auf Vergessenwerden" ausgeprägtere Löschungs-[2] und Berichtigungsansprüche[3] gewährt sowie ein neuer Anspruch auf „Datenportabilität" formuliert,[4] mit dem langfristig die Häufigkeit von Neuerhebungen personenbezogener Daten reduziert werden soll. Die für die Verarbeitung verantwortlichen Unternehmen müssen ihrerseits Instrumente und Verfahren entwickeln, die eine Datenschutz-Folgenabschätzung[5] ermöglichen. Neben diesen Instrumenten und Ansprüchen enthält die DS-GVO eine Reihe von vertrauten Strukturen, wie beispielsweise den Grundsatz des Verbots mit Erlaubnisvorbehalt,[6] und eine Vielzahl an Präzisierungen bisheriger datenschutzrechtlicher Prinzipien[7], die durchaus eine Überprüfung bestehender datenschutzrechtlicher Strukturen in Unternehmen auf ihre künftige Vereinbarkeit mit den Anforderungen der DS-GVO rechtfertigen.[8] Auch der Aufgabenbereich des Datenschutzbeauftragten ändert sich unter der DS-GVO, da die Verordnung dem betrieblichen Datenschutzbeauftragten eine stärkere Rolle[9] zuweist und diese nicht zuletzt auch im Zusammenhang mit der Einrichtung eines effektiven Systems der Datenschutz-Folgenabschätzung[10] sowie der Implementierung eines effektiven Datenschutz-Managementsystems an Bedeutung gewinnt.

Schließlich ist auf die mit der DS-GVO deutlich verschärften Bußgeldtatbestände des Art. 83 DS-GVO hinzuweisen, mit denen die Einhaltung des Datenschutzes noch stärker in den Fokus der Unternehmensführung und letztlich auch der Compliance rückt.

II. Die grundrechtliche Verankerung des Datenschutzrechts im nationalen und europäischen Recht

Personenbezogene Daten werden nach dem Volkszählungsurteil des Bundesverfassungsgerichts durch das Recht auf informationelle Selbstbestimmung verfassungsrechtlich geschützt: die Befugnis, über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen.[11] Das Recht auf informationelle Selbstbestimmung ist dabei keine „Erfindung" des Bundesverfassungsge-

---

der erste Rang eingeräumt wird, während die bisherige nationale Rechtslage strukturell unverändert (weiter) neben dem neu gefassten BDSG abgebildet bleibt.

[1] Vgl. Art. 25 DS-GVO.
[2] Vgl. Art. 17 DS-GVO.
[3] Vgl. Art. 16 DS-GVO.
[4] Vgl. Art. 20 DS-GVO.
[5] Art. 35 DS-GVO.
[6] Art. 6 DS-GVO.
[7] Siehe hierzu insbesondere die in Art. 5 Abs. 1 DS-GVO enthaltenen Grundsätze für die Verarbeitung personenbezogener Daten, deren Einhaltung von den Bußgeldtatbeständen des Art. 83 DS-GVO umfasst ist.
[8] Eine solche Überprüfung und Dokumentation der Einhaltung der Grundsätze nach Art. 5 Abs. 1 DS-GVO ist nicht zuletzt durch die in Art. 5 Abs. 2 DS-GVO fixierte Rechenschaftspflicht geboten.
[9] Siehe hierzu Art. 38 und 39 DS-GVO.
[10] Siehe hierzu Art. 35 DS-GVO.
[11] *BVerfGE* 65, 1 (41 ff.).

richts, sondern vielmehr eine „Konkretisierung" dessen, was bereits verfassungsrechtlich im allgemeinen Persönlichkeitsrecht verankert ist.[1] Das Bundesverfassungsgericht verdeutlicht im Volkszählungsurteil, dass es das informationelle Selbstbestimmungsrecht nicht in einer sphärenbezogenen Weise interpretiert, sondern dass dieses Recht vor Gefahren schützt, die sich aus der Zusammenfügung mit anderen Datensammlungen zu einem mehr oder weniger vollständigen Persönlichkeitsbild ergeben, dessen Richtigkeit und Verwendung der Betroffene nur unzureichend kontrollieren kann.[2] Damit entfaltet das Recht auf informationelle Selbstbestimmung einen flexiblen, gegenüber technischen und gesellschaftlichen Entwicklungen reagiblen und an der konkreten Gefährdungssituation ausgerichteten Gewährleistungsgehalt.[3] Als absolutes Nutzungs- und Verfügungsrecht analog dem Eigentum ist das informationelle Selbstbestimmungsrecht jedoch nicht anerkannt.[4] Die Konstruktion als absolutes Nutzungs- und Verfügungsrecht gilt als nicht angemessen, da der Betroffene kein Herrschaftsrecht über Informationen beanspruchen kann, die erst der Verwender aus einem Bestand von Daten konstruiert hat.[5] Schutzwürdig ist aber sein Recht, die Verwendung seiner persönlichen Daten durch Dritte kennen und kontrollieren zu können.[6] Das Bundesverfassungsgericht findet im Jahr 1983 hierfür noch deutliche Worte: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."[7]

Dies gilt besonders dann, wenn diese Verwendung sich für ihn selbst als folgenreich erweist. Denn nicht allein Art und Umfang der erhobenen Daten sind grundrechtsrelevant, vielmehr kommt es auch auf die denkbaren Verwendungen und das jeweilige Missbrauchspotential an.[8]

Eine erweiternde Interpretation hat das informationelle Selbstbestimmungsrecht durch das Urteil des Bundesverfassungsgerichts vom 2. März 2006 und den Beschluss vom 4. April 2006 erhalten. Mit dem Urteil des Zweiten Senats vom 2. März 2006[9] wurde die Grenze zwischen Fernmeldegeheimnis des Art. 10 GG und dem informationellen Selbstbestimmungsrecht nach Art. 1 Abs. 2 i. V. m. Art. 2 Abs. 1 GG gezogen. Der Schutz des Fernmeldegeheimnisses gilt nur für die telekommunikative Übermittlungsphase. Die auf Telekommunikationsendgeräten gespeicherten Daten werden hingegen durch das informationelle Selbstbestimmungsrecht geschützt. Nach diesem Schutzrecht ist den staatlichen Sicherheitsbehörden der Zugriff auf mobile Speichermedien verwehrt, wenn die dort gespeicherten Daten auf andere Weise schon verfügbar waren und der Eingriff damit nicht mehr für die Rechtssicherung notwendig war. Mit Beschluss vom 4. April 2006[10] zur Rasterfahndung hat der Erste Senat

---

[1] Vgl. instruktiv *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 45 f.
[2] *BVerfGE* 65, 1 (42).
[3] Auf die Gefährdungsabhängigkeit stellt *Trute,* Verfassungsrechtliche Grundlagen, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 156 ff., Rn. 14, ab.
[4] So aber *Ladeur,* DuD 2000, 12 (18).
[5] *Trute,* Verfassungsrechtliche Grundlagen, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 156 ff., Rn. 21.
[6] *Trute,* Verfassungsrechtliche Grundlagen, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 156 ff., Rn. 19.
[7] *BVerfGE* 65, 1 = NJW 1984, 419 (422).
[8] Vgl. *BVerfGE* 65, 1 (46).
[9] MMR 2006, 217.
[10] MMR 2006, 531.

des Bundesverfassungsgerichts eine Grenze für die polizeiliche Rasterfahndung gezogen.[1]

Nach Ansicht des Gerichts ist ein derart intensiver Grundrechtseingriff nur verhältnismäßig, wenn die Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts und die Nähe des Betroffenen zur Bedrohung eingegrenzt werden. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient. Die Maßnahme der Rasterfahndung zur Aufdeckung sog. „Schläfer" ist nur dann mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar, wenn eine „konkrete" und somit durch hinreichende Tatsachen zu belegende Gefahr für hochrangige Rechtsgüter, wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Das Vorliegen einer allgemeinen Bedrohungslage, etwa bei Vorliegen von vagen Vermutungen ohne greifbaren auf den Einzelfall bezogenen Anlass, ist hingegen nicht ausreichend.

Das Bundesverfassungsgericht hat mit seinem Urteil vom 27. Februar 2008 (1 BvR 370/07)[2] die rechtlichen Grenzen für heimliche Online-Durchsuchungen von Computern aufgezeigt.[3] Danach umfasst das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Diese neu interpretierte Ausprägung des allgemeinen Persönlichkeitsrechts soll vor Eingriffen in informationstechnische Systeme schützen, soweit der Schutz nicht durch andere Grundrechte, wie Art. 10, 13 GG und das Recht auf informationelle Selbstbestimmung gewährleistet ist. Das Grundrecht soll das Persönlichkeitsrecht vor den Gefahren schützen, die durch den Zugriff staatlicher Stellen auf vernetzte Systeme, wie PCs, Notebooks und Mobiltelefone, bestehen und deren Daten ein Bild über die Persönlichkeit des Nutzers bilden können. Es bleibt abzuwarten, ob dieses Grundrecht über die Rechtsfigur der mittelbaren Drittwirkung in den Privatrechtsbereich ausstrahlen wird wie auf die Überwachung von IT-Systemen, die Unternehmen ihren Mitarbeitern zur Verfügung stellen. Hierfür ist die Überwachung des E-Mail-Accounts, der auch für private Zwecke genutzt wird, ein Beispiel.

Das Bundesverfassungsgericht hatte in einer viel beachteten Entscheidung zu prüfen, ob die Umsetzung der Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden,[4] in das nationale Recht mit den verfassungsrechtlichen Vorgaben des Grundgesetzes vereinbar ist. Während der Europäische Gerichtshof zunächst noch in seiner Entscheidung vom 10. Februar 2009 (Rs. C-301/06) feststellte, dass die Richtlinie zu Recht auf der Grundlage des EG-Vertrages erlassen sei,[5] setzte sich das Bundesverfassungsgericht materiellrechtlich mit der Umsetzung der EG-Richtlinie über

---

[1] Vgl. *BVerfG*, ZD 2013, 328 m. Anm. *Petri*. Zur Konsequenz dieser Entscheidung für die Antiterrordatei *Kirchberg,* CR 2007, 10 (14); *Petri*, ZD 2013, 3; *ders.*, ZD 2014, 599; Rasterfahndung wegen Kinderpornographie soll den Anforderungen dieser Entscheidung entsprechen, da nur nach Straftätern gefahndet wird; hierzu FAZ v. 11. Januar 2007, S. 7 und 9.

[2] MMR 2008, 315 m. Anm. *Bär* = NJW 2008, 822.

[3] Siehe hierzu *Hornung,* CR 2008, 299; *Stögmüller,* CR 2008, 435.

[4] ABl. EG L 105, S. 54.

[5] *EuGH,* Urt. v. 10.2.2009, Rs. C-301/06, MMR 2009, 244.

Vorratsdatenspeicherung auseinander und kam zu dem Ergebnis, dass eine sechsmonatige anlasslose Speicherung von Telekommunikations-Verkehrsdaten mit Art. 10 GG schlechthin nicht vereinbar sei und es auf einen etwaigen Vorrang der EG-Richtlinie nicht ankomme.[1] Der EuGH selbst befand in seinem Urteil vom 8. April 2010, dass die Richtlinie mit dem geltenden EU-Recht nicht vereinbar sei, da der Eingriff in die nach Art. 7 und 8 Grundrechtecharta geschützten Rechte nicht verhältnismäßig sei.[2] Damit stellt der EuGH klar, dass auch das legislative Handeln der Organe der Europäischen Union an den in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte, zu denen ausdrücklich auch der Datenschutz zu rechnen ist, gemessen werden muss.[3]

Mit Beschluss vom 28. Oktober 2014 legte der BGH[4] dem EuGH im Rahmen eines Vorabentscheidungsverfahrens nach Art. 267 AEUV die Frage vor, ob Art. 2 Buchst. a) der EG-Datenschutzrichtlinie (RL 95/46/EG) so auszulegen ist, dass eine IP-Adresse bereits dann als personenbezogenes Datum anzusehen ist, wenn ein Dritter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt. Die Entscheidung des EuGH[5] stellt darauf ab, dass bei einer dynamischen IP-Adresse dann von einem personenbezogenen Datum auszugehen ist, wenn der Verantwortliche über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen. Mit der Entscheidung wird Rechtssicherheit für die Nutzung des Internets sowie der cloud-basierten Dienste geschaffen. Die Entscheidung behält auch für die Anwendung der DS-GVO ihre Bedeutung, da aus ihr deutlich wird, dass die Beurteilung der Frage, ob personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO im konkreten Fall vorliegen, stets aus der Perspektive dessen vorzunehmen ist, der mit diesem Datum eine Verarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO beabsichtigt.

Im europäischen Recht ist der Schutz des allgemeinen Persönlichkeitsrechts spätestens mit der Richtlinie 95/46/EG vom 24. Oktober 1995 (EG-Datenschutzrichtlinie) verankert. Während der EuGH zunächst zur Begründung des Datenschutzrechts auf allgemeine Rechtsgrundsätze zurückgreifen musste,[6] ist der Schutz personenbezogener Daten seit dem Inkrafttreten des Vertrags von Lissabon im Dezember 2009 im Primärrecht (EU-Verfassungsrecht) verankert. Art. 16 AEUV ist die Grundlage des heutigen europäischen Datenschutzrechts ebenso wie Art. 7 GRCh (Achtung des Privat- und Familienlebens) sowie Art. 8 GRCh (Schutz personenbezogener Daten).[7]

---

[1] *BVerfG,* Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, MMR 2010, 356.
[2] *EuGH,* Urt. v. 8.4.2014, Rs. C-203/12, C-594/12 (Digital Rights Ireland Ltd.), ZD 2014, 296 m. Anm. *Petri*.
[3] ABl. EG C 364, S. 1 v. 18.12.2000.
[4] *BGH,* Beschl. v. 28.10.2014 – VI ZR 135/13, GRUR 2015, 192.
[5] *EuGH,* GRUR Int. 2016, 1169 (Breyer) = NJW 2016, 3579 m. Anm. *Mantz/Spittka* = MMR 2016, 842 m. Anm. *Moos/Rothkegel* = ZD 2017, 24 m. Anm. *Kühling/Klar*.
[6] *EuGH,* Urt. v. 17.6.2014, verb. Rs. C-141/12 u. C-372/12 (Y. S. u. M. S./Minister voor Immigratie), EuR 2015, 89 m. Anm. *Gundel*.
[7] Siehe hierzu auch *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 1 ff.

III. Das Verhältnis des europäischen zum nationalen Datenschutzrecht

1. Europäische Richtlinie, Datenschutz-Grundverordnung und BDSG

Der Ministerrat und das Europäische Parlament verabschiedeten am 24. Oktober 1995 eine allgemeine Datenschutzrichtlinie, die in nationales Recht umgesetzt wurde.[1] Die mit der EG-Datenschutzrichtlinie bezweckte Harmonisierung des Datenschutzrechts in der Europäischen Union war bereits durch das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" (Europäische Datenschutzkonvention) vom 28. Januar 1981[2] (**Nr. 5**) vorgezeichnet. Die Konvention verpflichtete die Unterzeichnerstaaten, die niedergelegten Grundsätze als gemeinsames datenschutzrechtliches Minimum zu verwirklichen. Eine Pflicht der Mitgliedstaaten zur Umsetzung in nationales Recht war hiermit jedoch nicht verbunden. Eine solche Verpflichtung ist erst mit der allgemeinen Datenschutzrichtlinie des Jahres 1995 entstanden.

Der von der EU-Kommission am 25. Januar 2012 vorgelegte Entwurf einer Datenschutz-Grundverordnung sowie einer Richtlinie für die polizeiliche und justizielle Informationsverarbeitung[3] wurde als „Datenschutzpaket" im Gesetzgebungsverfahren nach Art. 294 AEUV intensiv und kontrovers diskutiert und erlebte mehrere teilweise tiefgreifenden Änderungen. Die schließlich verabschiedete DS-GVO spiegelt den politischen Kompromiss wider, der zwischen Kommission, Parlament und Rat gefunden wurde. Am 28. April 2016 wurde das Datenschutzpaket verabschiedet. Die DS-GVO trat am 25. Mai 2016 in Kraft und entfaltete ihre Wirksamkeit nach Art. 99 Abs. 2 DS-GVO am 25. Mai 2018.

a) Rechtsangleichung im Binnenmarkt

Die datenschutzrechtlichen Regelungen in Europa spiegeln die schrittweise Rechtsangleichung im Binnenmarkt und veranschaulichen zugleich das Verhältnis zwischen Europäischer Union einerseits und den Mitgliedstaaten andererseits. Während als Rechtsgrundlage für die Datenschutz-Richtlinie des Jahres 1995 die Notwendigkeit der Rechtsangleichung im Binnenmarkt (Art. 100a EGV) erachtet wurde, bildet vor allen Dingen Art. 16 AEUV, der ein eigenständiges Recht „jeder Person (…) auf Schutz der sie betreffenden personenbezogenen Daten" enthält, die Rechtsgrundlage zur Verabschiedung der DS-GVO. Darüber hinaus kann die DS-GVO auf Art. 8 Abs. 1 der Charta der Grundrechte der EU gestützt werden.[4] Nach dem Subsidiaritätsprinzip (Art. 5 Abs. 1 Satz 2 EUV) wird die EU nur dann tätig,[5] sofern und soweit ein Ziel besser auf der Gemeinschaftsebene als auf derjenigen der einzelnen Mitglied-

---

[1] *Ehmann/Helfrich,* EG-Datenschutzrichtlinie, Kurzkommentar, 1999.

[2] Hierzu näher *Burkert* in: Roßnagel, Handbuch Datenschutzrecht, 2.3 Internationale Grundlagen, Rn. 35.

[3] KOM(2012) 10 endg. v. 15.1.2012.

[4] Charta der Grundrechte der Europäischen Union vom 14.12.2007, ABl. Nr. C 303, S. 1.

[5] Die Tätigkeit der EU im Rahmen des Subsidiaritätsprinzips erfolgt über Art. 5 Abs. 1, 3 EUV hinaus auf der Grundlage des Protokolls über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit vom 13.12.2007, ABl. Nr. C 306, S. 150.

staaten erreicht werden kann.[1] Aus ökonomischer Sicht erfordert der Warenverkehr oder die Anbahnung und Abwicklung von Dienstleistungen eine europäische Regelung für die Verarbeitung personenbezogener Daten, da die Übermittlung personenbezogener Daten wesentlicher Bestandteil des Geschäftsverkehrs ist.

Datenschutz ist zugleich auch die Gewährleistung eines elementaren Menschenrechts. Der Gerichtshof hat das in Art. 8 der Europäischen Menschenrechtskonvention (EMRK) verankerte Recht auf Achtung des Privatlebens in seiner Entscheidung vom 5. Oktober 1994 als „ein von der Gemeinschaftsordnung geschütztes Grundrecht" bezeichnet und damit auch den Wert des Grundrechts auf Privatheit/Datenschutz für die Gemeinschaftsordnung betont. Zweck der RL 95/46/EG war es,[2] ein möglichst hohes und gleichwertiges Datenschutzniveau für den Binnenmarkt herzustellen. Diesem Ziel ist auch die DS-GVO verpflichtet. Sie nimmt in Erwägungsgrund 3 auf die RL 95/46/EG Bezug und betont die Gewährleistung eines hohen Datenschutzniveaus vor dem Hintergrund eines deutlich angestiegenen grenzüberschreitenden Datenverkehrs sowie der raschen technologischen Entwicklung und der mit der Globalisierung verbundenen datenschutzrechtlichen Herausforderungen.

Sowohl die Richtlinie als auch die DS-GVO regeln die manuelle und die automatisierte bzw. teilweise automatisierte Verarbeitung personenbezogener Daten in Dateien[3] bzw. Dateisystemen[4]. Die Definitionen, was unter „Datei" sowie „Dateisystem" zu verstehen ist, gehen weiter als jene des BDSG und erfassen „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird".[5]

Die DS-GVO[6] sieht unabhängige[7] Kontrollinstanzen (Aufsichtsbehörden) vor, die eine Regelkontrolle[8] vornehmen müssen.

Den Verantwortlichen für die Datenverarbeitung gab die RL 95/46/EG noch ein Wahlrecht zwischen der generellen Meldepflicht automatisierter Datenverarbeitung an ein öffentliches Register und der Bestellung eines betrieblichen/behördlichen Beauftragten für den Datenschutz.[9] Die DS-GVO kennt keine allgemeine Meldepflicht des Verantwortlichen[10] gegenüber einer Aufsichtsbehörde. Eine spezielle Meldepflicht sieht die DS-GVO allerdings für den Fall der Verletzung des Datenschutzes vor (Art. 33 DS-GVO). Die Einführung eines obligatorischen betrieblichen Datenschutzbeauftragten war im Rahmen der Verhandlungen über die DS-GVO zunächst noch umstritten. Während der Entwurf der Kommission vorsah, dass die Verantwortlichen für die Datenverarbeitung zur Bestellung eine betrieblichen Datenschutzbeauftragten verpflichtet werden sollten und sich das Europaparlament dieser Auffassung grundsätzlich

---

[1] Art. 5 Abs. 3 EUV.
[2] Erwägungsgrund 10 RL 95/46/EG.
[3] Art. 2 lit. c RL 95/46/EG.
[4] Art. 4 Nr. 6 DS-GVO.
[5] Art. 2 lit. c RL 95/46/EG sowie Art. 4 Nr. 6 DS-GVO; hierzu *Brühann* in: Roßnagel, Handbuch Datenschutzrecht, 2.4 Europarechtliche Grundlagen, Rn. 17–56.
[6] Art. 51 ff. DS-GVO.
[7] Art. 52 Abs. 1 DS-GVO.
[8] Art. 57 DS-GVO legt einen umfangreichen Katalog an Aufgaben fest, die durch die Aufsichtsbehörden wahrzunehmen sind.
[9] Art. 18 RL 95/46/EG.
[10] Art. 4 Nr. 7 DS-GVO.

anschloss, konnte sich der Rat auf eine solche Bestellungspflicht nicht einigen und sah vor, dass die Frage der obligatorischen Bestellung eines Datenschutzbeauftragten in der Regelungskompetenz der Mitgliedstaaten verbleiben solle.[1] Die DS-GVO sieht nun europaweit die Benennung eines Datenschutzbeauftragten vor, wenn bestimmte eng umschriebene Bedingungen vorliegen.[2] Darüber hinaus überlässt die DS-GVO es den Mitgliedstaaten, weitere Bedingungen vorzusehen, unter denen ein Datenschutzbeauftragter zu benennen ist.[3] Von dieser Regelungsbefugnis hat der Bundesgesetzgeber Gebrauch gemacht und mit § 38 Abs. 1 BDSG eine Verpflichtung zur Benennung eines Datenschutzbeauftragten vorgesehen, sofern zwanzig oder mehr Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, eine Datenschutz-Folgenabschätzung vorzunehmen ist oder Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Mit der Einrichtung eines Europäischen Datenschutzausschusses[4] nach Art. 68 DS-GVO ist die bislang unter der RL 95/46/EG eingerichtete Gruppe nach Art. 29 abgelöst. Dieser Ausschuss ist mit eigener Rechtspersönlichkeit ausgestattet,[5] übt seine Funktion unabhängig aus und findet seine Aufgabe in der Sicherstellung der einheitlichen Anwendung der DS-GVO.[6] Er füllt diese Aufgabe unabhängig von den durch die nationalen Aufsichtsbehörden wahrgenommenen Funktionen aus. Wie bereits im Fall der Gruppe nach Art. 29[7] wird auch der Europäische Datenschutzausschuss eine wichtige Rolle bei der Entwicklung von Leitlinien, Empfehlungen oder ähnlichen Verfahren einnehmen, die für die Datenschutzpraxis von Bedeutung sind.

b) Marktortprinzip, Anwendbarkeit des europäischen Datenschutzrechts und grenzüberschreitender Datenaustausch

Der Ort der Niederlassung wird von der DS-GVO[8] als Anknüpfungspunkt für die Anwendbarkeit des europäischen Datenschutzrechts bestimmt.[9] Die jeweiligen Datenschutzbestimmungen greifen also dort, wo die datenverarbeitende Stelle ihren Sitz hat. Das mit der DS-GVO in das Datenschutzrecht integrierte Marktortprinzip[10] führt dazu, dass auch dann die Bestimmungen der Verordnung zu beachten sind, wenn der Verarbeiter zwar seine Niederlassung nicht in der

---

[1] Vgl. zum Verlauf des Gesetzgebungsverfahrens die beim Bayerischen Landesamt für Datenschutzaufsicht unter www.lda.bayern.de erhältliche „Trilog-Synopse der DS-GVO".

[2] Art. 37 Abs. 1 lit. b und c DS-GVO.

[3] Art. 37 Abs. 4 DS-GVO.

[4] Vgl. https://edpb.europa.eu.

[5] Art. 68 Abs. 1 DS-GVO.

[6] Der Europäische Datenschutzausschuss informiert sowohl über die von ihm ausgeübten Tätigkeiten als auch über wichtige datenschutzrechtliche Entwicklungen unter https://edpb.europa.eu.

[7] Die Dokumente der Artikel-29-Datenschutzgruppe sind über einen Webserver der Europäischen Kommission zugänglich unter https://ec.europa.eu/info/law/law-topic/data-protection_de.

[8] Art. 3 Abs. 1 DS-GVO.

[9] Mit der DS-GVO wird dieses Prinzip in Art. 5 Abs. 2 DS-GVO um das Marktortprinzip ergänzt. Demzufolge findet die Verordnung auch dann Anwendung, wenn diese durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter erfolgt und die Datenverarbeitung im Zusammenhang damit steht, der betroffenen Person „in der Union Waren oder Dienstleistungen anzubieten" oder „das Verhalten Betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt".

[10] Hierzu eingehend *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 23 ff.; *Zerdick* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 2 ff.

Union hat, er aber gegenüber der betroffenen Person in der Union Waren oder Dienstleistungen anbietet (Art. 3 Abs. 2 lit. a DS-GVO). Entsprechendes gilt, wenn der nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeiter das Verhalten betroffener Personen beobachtet, soweit dieses Verhalten in der Union erfolgt. Damit fallen regelmäßig Tracking, Profiling oder auch Methoden der Verhaltensanalyse von Betroffenen auch dann in den Anwendungsbereich der DS-GVO, wenn der betreffende Anbieter nicht in der EU ansässig ist.

Der Datenexport in Drittstaaten ist nur im Rahmen der durch die europäischen Datenschutzbestimmungen vorgegebenen Grenzen zulässig. Das europäische Datenschutzrecht erlaubt den Datentransfer grundsätzlich nur dann, wenn im Land des Datenempfängers ein angemessenes Datenschutzniveau vorliegt.[1] Alternativ kann in Ausnahmefällen der Transfer vertraglich zwischen Datenübermittler, Betroffenem und Datenempfänger vereinbart werden (Vertragslösung), wenn auf diese Weise die datenschutzrechtlichen Interessen des Betroffenen durch die Übernahme geeigneter Garantien[2] sichergestellt werden. Für die Beurteilung des Schutzniveaus in der Gemeinschaft und in Drittstaaten spielte die Artikel-29-Datenschutzgruppe bislang eine wichtige Rolle. Sie nahm hierzu auf Anfrage gegenüber der Kommission Stellung, hat aber auch die Möglichkeit von sich aus präventiv Empfehlungen abzugeben.[3] Diese Funktion hat nun der Europäische Datenschutzausschuss nach Art. 68 DS-GVO übernommen. Die während der Geltungsdauer der RL 95/46/EG durch die Kommission gemäß Art. 25 Abs. 6 RL 95/46/EG getroffenen Feststellungen zu einem angemessenen Schutzniveau in bestimmten Drittländern bleiben auch nach dem Wirksamwerden der DS-GVO und der Ablösung der RL 95/46/EG nach Art. 45 Abs. 9 DS-GVO so lange in Kraft, bis sie durch einen nach Art. 45 Abs. 3 oder 5 DS-GVO erlassenen neuen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden. Ebenso bleiben die von der Kommission auf der Grundlage von Art. 26 Abs. 4 RL 95/46/EG verabschiedeten Standardvertragsklauseln **(Nr. 37–39)** in Kraft, bis sie durch einen neuerlichen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden (Art. 46 Abs. 5 DS-GVO). Mit dem „Privacy Shield"-Abkommen[4] bestand eine Nachfolgeregelung zu „Safe Harbor", die mit der Entscheidung des EuGH[5] nicht mehr als Grundlage für den Datenexport an in den USA ansässige Unternehmen dienen kann.

Das frühere BDSG wurde seit seinem Bestehen wiederholt Novellen unterzogen, die teilweise der technischen Entwicklung, ganz überwiegend jedoch der Umsetzung europäischer Richtlinienvorgaben geschuldet waren. Das BDSG hat darüber hinaus als Umsetzung der europäischen Vorgaben auch die

---

[1] Art. 45 Abs. 1 DS-GVO. Vgl. hierzu die wegweisende Rechtsprechung des *EuGH*, Urt. v. 16.7.2020 – C-311/18 (Schrems II), NJW 2020, 2613 = MMR 2020, 597 m. Anm. *Hoeren* = ZD 2020, 511 m. Anm. *Moos/Rothkegel*.

[2] Art. 46 DS-GVO.

[3] *Brühann* in: Roßnagel, Handbuch Datenschutzrecht, 2.4 Europarechtliche Grundlagen, Rn. 50–55.

[4] Siehe Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. EU L 207 v. 1.8.2016, S. 1.

[5] Vgl. *EuGH*, Urt. v. 16.7.2020 – C-311/18 (Schrems II), NJW 2020, 2613 = MMR 2020, 597 m. Anm. *Hoeren* = ZD 2020, 511 m. Anm. *Moos/Rothkegel* sowie bereits zuvor zur Kritik am Privacy Shield-Abkommen *Molnár-Gábor/Kaffenberger*, ZD 2017, 18; *Filip*, ZD-Aktuell 2016, 05108; *Weichert*, ZD 2016, 209. Allgemein zur Problematik des Datenverkehrs mit in den USA ansässigen Stellen *Spies* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2. Aufl., V.2. Rn. 9 ff.

durch die Europäische Grundrechtecharta geprägte Vorstellung vom Schutz des allgemeinen Persönlichkeitsrechts zu beachten. Diese Orientierung an der in der Europäischen Grundrechtecharta sowie der in Art. 16 EUV enthaltenen Gewährleistung des Rechts auf Schutz der personenbezogenen Daten in Europa wird das nationale Recht in verstärktem Maße nach dem Wirksamwerden der DS-GVO berücksichtigen müssen. Die DS-GVO entfaltet nach Art. 288 Abs. 2 AEUV allgemeine und unmittelbare Wirkung in den Mitgliedstaaten der EU. Sie verdrängt in der Praxis deshalb wegen des ihr innewohnenden Anwendungsvorrangs entgegenstehendes nationales Recht.[1]

2. Die Datenschutz-Grundverordnung

a) Rechtsnatur der DS-GVO

Bei der Datenschutz-Grundverordnung handelt es sich um eine europäische Verordnung nach Art. 288 Abs. 2 AEUV. Diese ist nach dem Wortlaut des AEUV unmittelbar anwendbar und bedarf ihrerseits keiner Umsetzung in den Mitgliedstaaten. Sie entspricht deshalb in ihrer Wirkung dem innerstaatlichen Gesetz.

Demgegenüber wäre eine Richtlinie nach Art. 288 Abs. 3 AEUV nur an die Mitgliedstaaten gerichtet und bezüglich der Ziele, wie sie in der Richtlinie verankert sind, für die Mitgliedstaaten bindend. Die Richtlinie bedarf deshalb der Umsetzung durch die Mitgliedstaaten, um gegenüber den EU-Bürgern Wirkung entfalten zu können.

Die Mitgliedstaaten haben im Rahmen der DS-GVO nur dort eine Möglichkeit, gesetzgeberisch tätig zu werden, wo dies die Verordnung selbst vorsieht. Entgegen der teilweise geäußerten Auffassung,[2] es gebe in der DS-GVO zahlreiche „Öffnungsklauseln", trifft dies nicht zu. Bereits der Wortlaut der DS-GVO zeigt klar und deutlich, dass die Mitgliedstaaten nur das Recht zur „Spezifizierung" der in der Verordnung enthaltenen Vorschriften haben.[3]

Es handelt sich also um Spezifizierungsklauseln.

Die Mitgliedstaaten können die in der Verordnung jeweils enthaltene Regelung genauer und auf einen Sachverhalt hin präzisieren. Dies gilt nicht generell sondern nur an jenen Stellen, an denen die Verordnung dies ausdrücklich zulässt.[4]

b) Verhältnis von DS-GVO zu BDSG

Die DS-GVO stellt die datenschutzrechtliche Grundlage für sämtliche Vorschriften dar, die den Schutz personenbezogener Daten bezwecken.[5] Sie enthält deshalb beispielsweise Rechtsgrundlagen für die Verarbeitung (z. B. Einwilligung)[6] oder auch eine Vorschrift, bei der das berechtigte Interessen des Verarbeiters[7] als Grundlage für die Verarbeitung herangezogen werden kann, wenn dies nach der Güterabwägung gegenüber dem Interesse des Betroffenen schwe-

---

[1] Vgl. statt vieler *Grabitz/Hilf/Nettesheim,* Das Recht der Europäischen Union, 71. EL August 2020, Art. 1 AEUV Rn. 79–81.

[2] Siehe hierzu *Heberlein* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 Rn. 6.

[3] Vgl. beispielsweise Art. 6 Abs. 2, Art. 6 Abs. 3 Satz 3, Art. 23 Abs. 2, Art. 88 Abs. 1 DS-GVO.

[4] Vgl. *Heberlein* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 Rn. 6.

[5] Art. 1 DS-GVO.

[6] Art. 6 Abs. 1 lit. a DS-GVO.

[7] Art. 6 Abs. 1 lit. f DS-GVO.

rer wiegt. Die DS-GVO enthält ferner zahlreiche Vorschriften, die sich sowohl mit der Art und Weise der Verarbeitung als auch der auf Seiten des Verantwortlichen oder des Auftragsverarbeiters vorzunehmenden Maßnahmen auseinandersetzen. In diesem Zusammenhang soll lediglich auf die Datenschutz-Folgenabschätzung[1] oder die Verpflichtung zur Erfüllung von Auskunftsansprüchen[2] sowie die Löschungsverpflichtung[3] hingewiesen werden.

Die Verordnung selbst enthält an einigen Stellen Spezifizierungsklauseln, mit denen die Mitgliedstaaten ermächtigt werden, speziellere Regelungen zur Ausformung der in der Verordnung enthaltenen Verpflichtungen zu erlassen. Dies gilt beispielsweise im Rahmen des Art. 88 DS-GVO für den Beschäftigtendatenschutz.

Zur Klärung des Verhältnisses zwischen DS-GVO und der nationalen Vorschrift, wie sie beispielsweise in BDSG enthalten sein könnte, ist die Rechtsprechung des Europäischen Gerichtshofs (EuGH)[4] zu beachten. Der EuGH hat mehrfach entschieden, dass eine schlichte Wiederholung europarechtlicher Vorschriften im nationalen Recht grundsätzlich nicht zulässig ist. Eine Wiederholung ist nach der Auffassung des EuGH in engen Grenzen nur dort zulässig, wo sie dem Ziel folgt, eine europarechtliche Vorschrift verständlicher zu machen. Grundsätzlich ist allerdings das „Wiederholungsverbot" durch den nationalen Gesetzgeber zu beachten und damit eine inhaltliche Wiederholung europarechtlicher Vorschriften folglich auf nationaler Ebene nicht gestattet. Ebenfalls ist nicht zulässig, dass der nationale Gesetzgeber mit eigenen Vorschriften den Geltungsbereich des Datenschutzrechts anders bestimmt, als dies mit der DS-GVO der Fall ist. Gänzlich unzulässig wäre die Regelung datenschutzrechtlicher Sachverhalte, die außerhalb der DS-GVO angesiedelt sind. Die europäische Datenschutz-Grundverordnung soll als umfassende Grundlage[5] den Schutz personenbezogener Daten regeln.

Die Gesetzgebung der Europäischen Union auf dem Gebiet des Datenschutzrechts beruht auf der in Art. 16 Abs. 2 AEUV verankerten Gesetzgebungskompetenz. Dabei handelt es sich um eine „geteilte Zuständigkeit" nach Art. 2 Abs. 2 AEUV i. V. m. Art. 4 Abs. 2 Buchst. j AEUV. Nach Art. 2 Abs. 2 Satz 2 AEUV nehmen die Mitgliedstaaten im Rahmen der geteilten Zuständigkeit ihre Kompetenz wahr, sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat.

Eine Regelungskompetenz der Mitgliedstaaten außerhalb der Vorschriften, wie sie in der DS-GVO angesiedelt sind, sieht die Verordnung nicht vor. Dies lässt sich bereits aus dem Wortlaut der Spezifizierungsklauseln ableiten, die klar nur davon sprechen, dass genauere Regelungen getroffen werden können. Dies schließt davon abweichende Regelungen aus, die ihrerseits im Konflikt zu der DS-GVO stehen könnten.

Es ist deshalb davon auszugehen, dass im Zweifel die DS-GVO anzuwenden ist. Nationale Regelungen können nur dann angewendet werden, wenn sie im

---

[1] Art. 35 DS-GVO.
[2] Art. 15 DS-GVO.
[3] Art. 17 DS-GVO.
[4] Siehe hierzu *Calliess/Ruffert*, EUV/AEUV, Art. 4 EUV Rn. 102; *Sydow*, DS-GVO, 2. Aufl., Einleitung, Rn. 37 f.; *EuGH,* Urt. v. 28.3.1985 – C 272/83, ECLI:EU:C:1985:147 Rn. 26 f. – Kommission/Italien; *EuGH,* Urt. v. 22.5.1975 – C-34/73, ECLI:EU:C:1973:101 = Slg. 1973, 981 = BeckEuRS 1973, 33732 = BeckRS 2004, 70873 Rn. 10 – Variola.
[5] Vgl. hierzu *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 82 ff.

Rahmen der europarechtlichen Zulässigkeit unter Beachtung der Spezifizierungsklauseln geschaffen wurden. Eine eigenständige Regelungskompetenz besteht auf nationaler Ebene nicht.

Nach der ständigen Rechtsprechung des Europäischen Gerichtshofs genießt das europäische Recht gegenüber dem nationalen Recht, sog. „Anwendungsvorrang“[1]. Im Rahmen der Gesetzgebungskompetenz der Europäischen Union geschaffenes Recht verdrängt nicht automatisch das bestehende nationale Recht in dem Sinne, dass das nationale Recht ungültig würde. Dies wäre allenfalls der Fall, wenn von einen sog. „Geltungsvorrang“ ausgegangen werden könnte.

Dies ist jedoch nach der Auffassung des EuGH[2] nicht der Fall, da die europäische Gesetzgebungskompetenz sich nicht auf die Aufhebung nationalen Rechts, das stets in der Gesetzgebungskompetenz der Mitgliedstaaten verbleibt, erstreckt und der Europäische Gerichtshof nicht zur Intervention[3] in die Rechtsprechung der Mitgliedstaaten befugt ist.

In der Praxis bringt dies die Schwierigkeit mit sich, dass im Einzelfall sowohl eine europarechtliche Vorschrift besteht als auch eine nationale Bestimmung den Anspruch formal erhebt, beachtet zu werden.

Der Rechtsanwender muss deshalb kritisch prüfen, ob das geltende nationale Recht gänzlich oder in Teilen gegen europäische Rechtsvorschriften verstößt. Ist dies der Fall, so ist der europäischen Vorschrift in der Anwendung der Vorrang zu gewähren.

c) Rechenschaftspflicht

Die DS-GVO enthält in Art. 5 Abs. 1 die Grundsätze der Datenverarbeitung. Über diese Grundsätze und deren Einhaltung muss der Verantwortliche nach Art. 5 Abs. 2 DS-GVO Rechenschaft ablegen (Accountability). Bei den Grundsätzen der Datenverarbeitung nach Art. 5 Abs. 1 DS-GVO handelt es sich um:

- Rechtmäßigkeit der Verarbeitung
- Verarbeitung nach Treu und Glauben
- Transparenz der Verarbeitung
- Zweckbindung der Verarbeitung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität
- Vertraulichkeit.

Über diese in der DS-GVO genannten Grundsätze der Datenverarbeitung muss der Verantwortliche im Rahmen seiner Rechenschaftspflicht den Nachweis erbringen, dass diese eingehalten werden. Kann dieser Nachweis nicht erbracht werden, droht ein Bußgeld nach Art. 83 Abs. 5 DS-GVO, das bis zu 20 Millionen Euro oder im Falle eines Unternehmens 4 Prozent seines Weltjahresumsatzes des vorausgegangenen Geschäftsjahres betragen kann, je nachdem, welcher der Beträge höher ist.

---

[1] *EuGH*, Urt. v. 28.3.1985 – Rs. 273/82, Slg. 1984, 483, Rn. 6; *Sydow*, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Einleitung, Rn. 36.

[2] Ebenda.

[3] Vgl. beispielsweise Art. 6 Abs. 2, Art. 6 Abs. 3 Satz 3, Art. 23 Abs. 2, Art. 88 Abs. 1 DS-GVO.

Eine genaue Auseinandersetzung mit diesen Prinzipien ist folglich zur Vermeidung des Bußgeldes dringend geboten. Der Gesetzgeber macht mit den in Art. 5 Abs. 1 DS-GVO enthaltenen Grundsätzen deutlich, dass derjenige, der personenbezogenen Daten verarbeitet, in besonders sorgsamer Weise mit den Daten umzugehen und den mit der Verarbeitung verbundenen Risiken Rechnung zu tragen hat.

d) Rechtmäßigkeit der Verarbeitung

Die Frage, unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen, ist in Art. 6 Abs. 1 DS-GVO abschließend geregelt. Mit der Struktur des Art. 6 Abs. 1 DS-GVO trifft die europäische Datenschutzgesetzgebung eine einheitliche Bestimmung, unter welchen Voraussetzungen die Verarbeitung rechtmäßig ist. Art. 6 Abs. 1 DS-GVO verkörpert das bereits im bisherigen nationalen Recht enthaltene „Verbot mit Erlaubnisvorbehalt". Demnach ist die Verarbeitung nur rechtmäßig, wenn eine der in Art. 6 Abs. 1 Buchst. a bis f DS-GVO genannten Bedingungen erfüllt ist. Die sind im Einzelnen:

(i) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.
(ii) Die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich, dessen Vertragspartei die betroffene Person ist. Ebenso ist die Verarbeitung rechtmäßig, wenn sie zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage des Betroffenen erfolgen.
(iii) Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt. Bei dieser rechtlichen Verpflichtung handelt es sich nicht um vertragliche Verpflichtungen, die sich aus dem Verhältnis zweier Parteien ergeben und die jeweilige Vertragspartei zu erfüllen hat. Der Gesetzgeber DS-GVO geht hier davon aus, dass es sich um rechtliche Verpflichtungen handelt, die durch Normen eines Gesetzgebers (formelle oder materielle Gesetze) resultieren.[1]
(iv) Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
(v) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt. Ebenso ist die Verarbeitung rechtmäßig, wenn sie in Ausübung einer öffentlichen Gewalt erforderlich ist, die dem Verantwortlichen, beispielsweise im Rahmen der Funktion als beliehener Unternehmer, übertragen wurde.
(vi) Die Verarbeitung ist zur Wahrnehmung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person die den Schutz bezugsbezogener Daten bezwecken, überwiegen.[2] Dies gilt insbesondere auch dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Im Zusammenhang mit der Rechtmäßigkeit der Verarbeitung ist in Art. 6 Abs. 2 DS-GVO eine der bereits genannten Spezifizierungsklauseln vorzufinden. Der europäische Gesetzgeber gestattet es den Mitgliedstaaten, spezifische Bestimmungen „zur Anpassung der Anwendung der Vorschriften dieser Ver-

---

[1] *Heberlein* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl., Art. 6 Rn. 15 ff.
[2] Siehe zur Güterabwägung insbesondere Erwägungsgrund 47 DS-GVO.

ordnung“ beizubehalten oder einzuführen. Diese Befugnis ist allerdings nur auf die in Art. 6 Abs. 1 Buchst. c und e DS-GVO enthaltenen Tatbestände beschränkt.

Dies bedeutet, dass der nationale Gesetzgeber spezifischere Regelungen aufstellen kann, die eine Verpflichtung zur Datenverarbeitung mit sich bringen. Dies ist beispielsweise dort erfolgt, wo handelsrechtliche Aufbewahrungspflichten eine Speicherung der Daten erfordern. Die insoweit einschlägige Vorschrift des Handelsgesetzbuches (HGB) wurde deshalb als **Nr. 35** in diese Textsammlung aufgenommen. Ebenso ist an sozialversicherungsrechtliche Regelungen oder steuerrechtliche Regelungen **(Nr. 36)** zu denken, die eine Datenverarbeitung als Pflicht beinhalten. Die Verabschiedung eines Patientendatenschutzgesetzes ist ebenso als aktuelles Beispiel zu nennen, das im Rahmen des Fünften Buches des Sozialgesetzbuches (SGB V) zu weitreichenden Änderungen geführt hat **(Nr. 27)**.

Soweit ein Mitgliedstaat Aufgaben wahrnimmt, die im öffentlichen Interesse liegen oder eine Ausübung öffentlicher Gewalt darstellen, lässt Art. 6 Abs. 2 DS-GVO dem Mitgliedstaat die Möglichkeit, die hierzu erforderlichen spezifischen Vorschriften zu erlassen. Entscheidend ist allerdings, dass diese im Rahmen der Spezifizierungsklauseln erlassenen Vorschriften tatsächlich die Anforderungen der DS-GVO präzise bestimmen und dem Zweck folgen, eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Für sog. „besondere Verarbeitungssituationen“ sieht bereits die DS-GVO Spezifizierungsklauseln in den Art. 85 bis 91 DS-GVO vor. Hierunter sind beispielsweise auch der Beschäftigtendatenschutz oder die Regelungen zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Meinungsäußerung und Informationsfreiheit zu rechnen.

e) Einwilligung

Im Rahmen des Art. 6 Abs. 1 Buchst. a DS-GVO kommt der Einwilligung als eigenständigem Erlaubnistatbestand eine besondere Bedeutung zu. Art. 4 Nr. 11 DS-GVO definiert die Einwilligung als jede freiwillig für den bestimmten Fall und in informierter Weise sowie unmissverständlich abgegebene Willensbekundung.[1)] Diese kann in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung (schlüssiges Verhalten) abgegeben werden. Ausschlaggebend ist allerdings, dass die betroffene Person mit dieser Erklärung zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Der Europäische Gerichtshof hat in einer weitreichend beachteten Entscheidung vom 1. Oktober 2019 deutlich gemacht, dass die Vorbelegung eines Ankreuzkästchens, das der Internetnutzer nicht abwählt, den Anforderungen an eine eindeutige bestätigende Handlung nicht genügt.[2)]

Die Einwilligung ist also eine Erklärung, die einen klaren unmissverständlichen Erklärungswillen beinhaltet, der sich auf die Verarbeitung der betreffenden Daten bezieht. Die Einwilligung ist eine „informierte Einwilligung“, da sich bereits denklogisch eine Einwilligung nur auf jene Sachverhalte erstrecken kann, über die der Erklärende ein Bewusstsein hat entwickeln können.

---

1) Siehe hierzu die Entscheidung des EuGH zu den Anforderungen an eine wirksame Einwilligung i. S. d. Art. 4 Nr. 11 DS-GVO, *EuGH,* Urt. v. 1.10.2019 – C-673/17 (Planet49), MMR 2019, 732 m. Anm. *Moos/Rothkegel* = ZD 2019, 556 m. Anm. *Hanloser.*

2) Ebenda.

Der Verantwortliche hat nach Art. 7 DS-GVO die Beweislast zu tragen, dass die erklärte Einwilligung den gesetzlichen Anforderungen genügt. Ebenso ist nach Art. 7 Abs. 2 DS-GVO das Ersuchen um Einwilligung in „verständlicher und leicht zugänglicher Form" sowie in einer „klaren und einfachen Sprache" so abzufassen, dass es von anderen Sachverhalten klar zu unterscheiden ist. Die DS-GVO gibt folglich einen Gestaltungsrahmen vor, der bei der Ausgestaltung des Einwilligungsprozesses zu beachten ist. Werden Teile der Einwilligungserklärung auf unklarer Basis abgegeben, sind sie nicht verbindlich, da sie als Verstoß gegen die Verordnung zu werten sind.

Der Betroffene hat jederzeit das Recht, seine Einwilligung zu widerrufen. Der Widerruf der Einwilligungserklärung bezieht sich allerdings nur auf die künftige Rechtmäßigkeit der Verarbeitung. Beruht eine in der Vergangenheit erfolgte Verarbeitung auf einer wirksamen Einwilligung, ist diese vom Widerruf nicht erfasst. Der Widerruf entfaltet nur Wirkung für die Zukunft. Der Betroffene muss vor der Abgabe seiner Einwilligungserklärung von seinem Widerrufsrecht in Kenntnis gesetzt werden. Ebenso ist der Widerruf der Einwilligung so einfach auszugestalten, wie dies für die Erteilung der Einwilligungserklärung vorgesehen ist.

Art. 7 Abs. 4 DS-GVO sieht schließlich ein Koppelungsverbot vor, wonach die Einwilligung, um noch als „freiwillige Einwilligung" klassifiziert werden zu können, nicht an die Erbringung einer anderen Leistung gekoppelt werden darf.

Art. 8 DS-GVO fixiert besondere Anforderungen für die Einwilligung, wie sie durch einen Minderjährigen erklärt werden. Die Gesetzesbestimmung sieht vor, dass ein Kind, das sein sechzehntes Lebensjahr noch nicht vollendet hat, nicht wirksam selbst einwilligen kann. Die Einwilligung ist nur rechtmäßig, sofern diese durch den „Träger der elterlichen Verantwortung" erklärt oder die Einwilligungserklärung mit dessen Zustimmung abgegeben wurde.

Mit der Einwilligung ist ein besonderes Haftungsrisiko verbunden: Art. 7 Abs. 1 DS-GVO legt dem Verantwortlichen die Beweislast auf. Art. 83 Abs. 5 Buchst. a DS-GVO sieht ein Bußgeld von bis zu 4 Prozent des Weltjahresumsatzes vor, sofern die Wirksamkeit der Einwilligung nicht gegeben ist.

Das Gesetz macht deutlich, dass die Einwilligung sich auf einen konkreten Verarbeitungszweck bezieht. Die Informationen, die der Verantwortliche dem Betroffenen im Rahmen des Einwilligungsprozesses zur Verfügung stellen muss, haben deshalb die Verarbeitungszwecke klar und hinreichend präzise zu umfassen.

Schließlich ist die Einwilligungserklärung zu dokumentieren und dafür zu sorgen, dass sowohl der Informationsfluss als auch Art und Umfang der Einwilligung hinreichend nachgewiesen werden können, um die Anforderungen des Art. 7 Abs. 1 DS-GVO zu erfüllen.

f) Rechte des Betroffenen – Pflichten des Verantwortlichen

Den Rechten des Betroffenen entsprechen regelmäßig auch korrespondierenden Pflichten des Verantwortlichen. An vorderster Stelle ist das aus Art. 12 DS-GVO abzuleitende Transparenzgebot zu nennen, da dort dem Verantwortlichen die Verpflichtung auferlegt wird, geeignete Maßnahmen zu treffen, um dem Betroffenen die Ausübung seiner Rechte zu ermöglichen.

Informationspflicht. Art. 12 DS-GVO beinhaltet über Art. 13 DS-GVO hinausgehende Informationspflichten, die der Verantwortliche zu erbringen hat.

Einführung

Art. 13 und 14 DS-GVO unterscheiden danach, ob die Erhebung personenbezogener Daten beim Betroffenen selbst oder indirekt erfolgt. In beiden Fallkonstellationen sind dem Betroffenen gesetzlich verankerte Informationen „entweder bei der Erhebung" oder innerhalb einer angemessenen kurzen Frist nach der Erhebung (längstens innerhalb eines Monats gemäß Art. 14 Abs. 3 Buchst. a DS-GVO) zu unterbreiten.

Auskunftsanspruch. Art. 15 DS-GVO sieht ein Auskunftsrecht der betroffenen Person vor. Dabei hat der Betroffene einen Anspruch darauf, dass ihm die Verarbeitungszwecke sowie die Kategorien der personenbezogenen Daten, die verarbeitet werden, mitgeteilt werden. Gleichfalls erstreckt sich das Auskunftsrecht auf die etwaigen Empfänger von Daten und auf die Frage, ob diese Empfänger möglicherweise in Drittländern ansässig sind.

Ebenso ist das Auskunftsrecht auf die Dauer der Verarbeitung (Speicherfristen, Löschungsbedingungen) zu erstrecken. Auf das Recht des Betroffenen, die Berichtigung der Daten oder Löschung zu verlangen, ist in diesem Zusammenhang ebenfalls hinzuweisen.

Eine besondere Verpflichtung besteht dahingehend, dem Betroffenen eine Information über das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde zu erteilen. Dies kann beispielsweise dadurch erfolgen, dass vorsorglich im Rahmen eines Impressums auf die entsprechende Aufsichtsbehörde hingewiesen wird.

Werden personenbezogene Daten indirekt, das heißt nicht bei der betroffenen Person selbst, erhoben, so erstreckt sich die Auskunftsverpflichtung auch auf die Herkunft der Daten. Ebenso muss die Auskunft das Bestehen einer automatisierten Entscheidungsfindung, sofern diese stattfindet, umfassen.

Problematisch ist die Verpflichtung nach Art. 15 Abs. 3 DS-GVO, eine Kopie „der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", dem Betroffenen zur Verfügung zu stellen.[1] Diese Kopie ist unentgeltlich zur Verfügung zu stellen. Eine Bearbeitungsgebühr kann nur dann verlangt werden, wenn es sich um eine wiederholte Anforderung einer Datenkopie handelt.

Das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 2 DS-GVO ist allerdings durch die Rechte und Freiheiten anderer Personen beschränkt (Art. 15 Abs. 4 DS-GVO).

Recht auf Vergessenwerden (Löschung). Die DS-GVO sieht in Art. 17 ein Recht auf Löschung vor. Landläufig wird dies als „Recht auf Vergessenwerden" bezeichnet. Die Tatbestandsvoraussetzungen für die Geltendmachung des Löschungsanspruchs sind in Art. 17 DS-GVO abschließend geregelt. Grundsätzlich kann davon ausgegangen werden, dass so lange nicht gelöscht werden muss, als im Rahmen des Art. 6 Abs. 1 DS-GVO der Verantwortliche eine Rechtsgrundlage für die weitere Verarbeitung bzw. Speicherung der Daten für sich in Anspruch nehmen kann.

Datenportabilität. Art. 20 DS-GVO sieht ein Recht auf Datenübertragbarkeit (Portabilität) vor. Dabei ist zu beachten, dass der Anspruch auf Erhalt der Daten in einem strukturierten, gängigen und maschinenlesbaren Format auf jene Daten beschränkt ist, die die betroffene Person dem Verarbeiter bereitgestellt hat. Denkbar wäre dies beispielsweise im Verhältnis des Versicherungsneh-

---

[1] Siehe hierzu die Entscheidung des *BAG* zum Umfang des Auskunftsanspruchs eines ausgeschiedenen Mitarbeiters gegen den ehemaligen Arbeitgeber, *BAG*, Urt. v. 27.4.2021 – 2 AZR 342/20 sowie zum Auskunftsanspruch des Betriebsrats, *BAG*, Beschl. v. 9.4.2019 – 1 ABR 51/17, ZD 2020, 46 m. Anm. *Tiedemann*.

mers zur Versicherungsgesellschaft, bei Nutzerdaten, die bei Geschäftsmodellen der Software as a Service (SaaS) anfallen oder beispielsweise bei Exportfunktionen proprietärer datenverarbeitender Systeme.

g) Datenschutzmanagementsystem

Art. 25 DS-GVO enthält die Verpflichtung des Verantwortlichen, seine Verarbeitungen nach den Grundprinzipien der „Privacy by Design" sowie der „Privacy by Default" auszurichten. Der Verantwortliche wird nach Art. 24 DS-GVO verpflichtet, präventive Maßnahmen zu ergreifen, die im Wesentlichen in der Vornahme geeigneter technischer und organisatorischer Maßnahmen liegen. Er hat dabei das Risiko zu berücksichtigen, das von der Art, dem Umfang, der Umstände sowie der Zwecke der Datenverarbeitung ausgeht und bei der Beurteilung des Risikos die Eintrittswahrscheinlichkeit sowie die Schwere eines Eingriffs in das Persönlichkeitsrecht zu berücksichtigen.

Die in Art. 24 und Art. 25 DS-GVO enthaltenen Grundsätze werden in den nachfolgenden Bestimmungen, insbesondere der Verpflichtung zur Aufstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO), der Sicherstellung der Sicherheit der Verarbeitung (auf Art. 32 DS-GVO) sowie der Vornahme der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) konkretisiert. Insgesamt ergeben diese Verpflichtungen im Zusammenhang mit der Pflicht zur Benennung eines Datenschutzbeauftragten ein Datenschutzmanagement-System, zu dessen Errichtung und Unterhaltung der Verantwortliche verpflichtet ist.

Entscheidend ist in diesem Zusammenhang, dass vor dem Hintergrund der Rechenschaftspflicht, wie sie in Art. 5 Abs. 2 DS-GVO verankert ist, der Verantwortliche den Nachweis über die Einhaltung der DS-GVO sowie die Überprüfung und Aktualisierung der von ihm ergriffenen Maßnahmen sicherzustellen hat.

h) Datenschutz-Folgenabschätzung

Art. 35 DS-GVO enthält die Verpflichtung zur Datenschutz-Folgenabschätzung. Diese ist nach Art. 35 Abs. 1 DS-GVO vorzunehmen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung „neuer Technologien" aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlichen zu einem hohen Risiko für die Beeinträchtigung der Rechte und Freiheiten natürlicher Personen führt.

Bedeutsam ist in diesem Zusammenhang, dass Art. 35 Abs. 1 DS-GVO mit dem Begriff „neue Technologien" auf eine allgemeine Betrachtung des Stands der Technik abstellt und nicht als Bezugsgröße den bisherigen Technologieeinsatz im Unternehmen selbst ansieht.[1)] Wird also im Unternehmen des Verarbeiters eine neue Technologie eingeführt, mit der sich die Risiken für die Verarbeitung personenbezogener Daten verändern, ist grundsätzlich eine Datenschutz-Folgenabschätzung, jedenfalls in ihren ersten Stufen, durchzuführen. Ziel ist dabei feststellen, ob ein hohes Risiko mit diesen Technologien verknüpft ist.

[1)] Vgl. hierzu *Baumgartner* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 35 Rn. 23 mit Verweis auf Erwägungsgrund 91; *Sassenberg/Schwendemann* in: Sydow, DS-GVO, 2. Aufl., Art. 35 Rn. 10.

Einführung

Auf den ersten Blick scheint die Vorschrift nur darauf abzustellen, dass ein hohes Risiko besteht und legt die Vermutung nahe, eine Datenschutz-Folgenabschätzung sei in allen anderen Fällen nicht durchzuführen. Diese Einschätzung ist jedoch bei genauer Betrachtung nicht zutreffend. Eine Folgenabschätzung ist jedenfalls insoweit durchzuführen, als überhaupt festgestellt werden muss, ob ein hohes Risiko für die Verarbeitung besteht. Sollte ein solches hohes Risiko bejaht werden, muss im Anschluss an die Folgenabschätzung danach gesucht werden, mit welchen Eindämmungsmaßnahmen das hohe Risiko reduziert werden kann.

In diesem Zusammenhang ist darauf hinzuweisen, dass in einem Fall, in dem ein hohes Risiko nicht eingedämmt werden kann, die Verarbeitung nicht schlechterdings verboten ist. Vielmehr hat der Verantwortliche nach Art. 36 DS-GVO die Aufsichtsbehörde zu konsultieren, um gemeinsam mit dieser nach möglichen Eindämmungsmaßnahmen zu suchen.

Die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist in vier Schritten durchzuführen.

(1) Zunächst ist eine systematische Beschreibung der Verarbeitungsvorgänge vorzunehmen (Art. 35 Abs. 7 Buchst. a DS-GVO). Diese systematische Beschreibung kann durchaus auf der Grundlage des nach Art. 30 DS-GVO zu erstellenden Verzeichnisses von Verarbeitungstätigkeiten vorgenommen werden. Gleichwohl bietet die DS-GVO die Möglichkeit, im Hinblick auf die Detailliertheit der Folgenabschätzung einen anderen Betrachtungsansatz zu wählen, als dies nach Art. 30 DS-GVO für das Verzeichnis der Verarbeitungstätigkeiten der Fall ist. Art. 35 Abs. 7 Buchst. a DS-GVO stellt auf die „geplanten Verarbeitungsvorgänge“ ab. Nach der Legaldefinition der Verarbeitung, wie sie in Art. 4 Nr. 2 DS-GVO vorzufinden ist, stellt eine Verarbeitung auch „Vorgangsreihen“ dar, die im Zusammenhang mit personenbezogenen Daten vorgenommen werden. Art. 35 DS-GVO lässt folglich durchaus zu, dass Geschäftsprozesse als Vorgangsreihen definiert werden, die sodann als Geschäftsprozesse selbst Gegenstand der Folgenabschätzung sind. Damit setzt die Datenschutz-Folgenabschätzung nicht alleine an einer juristischen Betrachtung der Verarbeitungsvorgänge an. Eine betriebswirtschaftlich differenzierte Analyse der Unternehmensabläufe gestattet hier eine ökonomische und effiziente Durchführung der Folgenabschätzung. Abstrakte Empfehlungen sind hier allerdings kaum möglich, da die Identifikation und Beschreibung von Geschäftsprozessen sowohl von den Geschäftsmodellen selbst als auch den Strukturen im Unternehmen abhängen.

(2) An die systematische Beschreibung schließt sich die Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Verarbeitungszweck an. Diese Stufe setzt sich mit der Rechtsgrundlage der Verarbeitung auseinander, wie sie in Art. 6 Abs. 1 DS-GVO enthalten ist. Bereits der Wortlaut der Bestimmung in Art. 35 Abs. 7 Buchst. b DS-GVO zeigt, dass eine Verhältnismäßigkeitsprüfung stattzufinden hat. Diese erfolgt nicht nur im Fall des Art. 6 Abs. 1 Buchst. f DS-GVO sondern auch in jenen Fällen, in denen beispielsweise aufgrund einer Einwilligung in Art. 6 Abs. 1 Buchst. a DS-GVO eine Verarbeitung erfolgen kann. Auch in diesem Fall ist der Verantwortliche nicht schlechterdings berechtigt, jede Art der Verarbeitung durchzuführen. Er hat vielmehr eine Verhältnismäßigkeitsprüfung vorzunehmen und jenes Mittel zur Verarbeitung zu wählen, das den geringsten Eingriff in die Persönlichkeitsrechte mit sich bringt.

(3) In der dritten Stufe der Folgenabschätzung erfolgt die eigentliche Risikobewertung für die Rechte und Freiheiten des Betroffenen. An dieser Risikoab-

schätzung, deren Verpflichtung auf der Ebene der Geschäftsleitung (Gesamtverantwortung nach Art. 35 Abs. 1 Satz 1 DS-GVO) liegt, nimmt die gesamte der Geschäftsleitung unterstellte Struktur des Unternehmens teil, da im Rahmen der Definition der Geschäftsprozesse die jeweiligen beteiligten Abteilungen einzubeziehen sind. Daneben ist der Datenschutzbeauftragte auf Anforderung der Geschäftsleitung nach Art. 35 Abs. 2 DS-GVO beratend hinzuzuziehen. Dies empfiehlt sich insbesondere im Hinblick auf die Prüfung der Verhältnismäßigkeit sowie die Durchführung der eigentlichen Risikofolgenabschätzung.

Diese Stufe setzt die Identifikation unternehmensspezifischer oder verarbeitungsspezifischer Bedrohungsszenarien voraus. Hier ist von Bedeutung, dass der Verantwortliche sich im Detail mit den möglichen Bedrohungsszenarien auseinandersetzt. Dies können sowohl Szenarien sein, wie sie sich aus einschlägigen ISO-Normen zur Datensicherheit ergeben. Daneben sind jedoch auch Bedrohungsszenarien vorstellbar und zu berücksichtigen, wie sie sich aus organisatorischen Risiken oder solchen des Geschäftsmodells ableiten lassen. Diese Bedrohungsszenarien sind im Rahmen einer Balanced-Score-Card aufzunehmen, um schließlich hieraus abgebildet eine Risikoeinschätzung vorzunehmen. Die Risikoeinschätzung ist an den Datenschutzzielen der Verfügbarkeit, Integrität und Vertraulichkeit zu orientieren. Diese Datenschutzziele ergeben sich sowohl aus Art. 5 Abs. 1 Buchst. f DS-GVO als auch aus Art. 32 Abs. 1 Buchst. b DS-GVO. Berücksichtigt man im Rahmen der Balanced-Score-Card die mögliche Auswirkung etwaiger Risikosituationen als auch jeweilige Eintrittswahrscheinlichkeit, ergeben sich im Hinblick auf die Datenschutzziele Wertepaare, die in einer Tabelle nach Risikoklassen abgebildet werden können.

(4) Ergibt diese Risikobewertung ein voraussichtlich hohes Risiko, so fordert Art. 35 Abs. 7 Buchst. d DS-GVO die Identifikation etwaiger Abhilfemaßnahmen, mit denen die Risiken so reduziert werden können, dass jedenfalls kein hohes Risiko vorliegt.

Sowohl die Risikofolgenabschätzung als auch die jeweiligen Abhilfemaßnahmen sind so zu dokumentieren, dass die Datenschutz-Folgenabschätzung und die hierauf gebildeten Maßnahmen der Aufsichtsbehörde vorgelegt werden können. Die Datenschutz-Folgenabschätzung ist kein einmaliger Vorgang. Die DS-GVO fordert in Art. 35 Abs. 11 eine Überprüfung der Wirksamkeit der Maßnahmen sowie dahingehend, ob die Verarbeitung auch tatsächlich gemäß der erfolgten Risikoabschätzung durchgeführt wird. Eine neuerliche Überprüfung ist jedenfalls dann erforderlich, wenn mit den Verarbeitungsvorgängen Änderungen verbunden sind, die sich auf das analysierte Risiko auswirken.

i) Datenschutzbeauftragter

Art. 37 DS-GVO verlangt die Benennung eines Datenschutzbeauftragten,[1] wenn die Verarbeitung einer Behörde oder öffentlichen Stelle durchgeführt wird (Art. 37 Abs. 1 Buchst. a DS-GVO) oder die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 Abs. 1 Buchst. b DS-GVO) der die Kerntätigkeit des Verantwortlichen oder des Auftragsverar-

[1] Siehe zu den Voraussetzungen der Benennung eines Datenschutzbeauftragten sowie dessen Stellung und Aufgaben die Kommentierung bei *Helfrich* in: Sydow, DS-GVO, 2. Aufl., Art. 37 ff.

beiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder Art. 10 DS-GVO besteht (Art. 37 Abs. 1 Buchst. c DS-GVO).

In diesen genannten Fällen besteht eine Benennungspflicht. Diese Pflicht knüpft nach der DS-GVO nur an diesen drei Fallgruppen an. Auf die Frage, wie viele Personen mit der Datenverarbeitung befasst sind oder inwieweit sich diese auswirkt, ist für die Pflicht nach der DS-GVO ohne Belang.

Zusätzlich zu der in Art. 37 Abs. 1 DS-GVO verankerten Benennungspflicht sieht § 38 BDSG vor, dass ein Datenschutzbeauftragter dann zu benennen ist, wenn mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung beschäftigt sind. Ebenso ist ein Datenschutzbeauftragter zu benennen, wenn es sich um eine Verarbeitung handelt, die der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO bedarf oder wenn geschäftsmäßig Daten verarbeitet werden oder dies zum Zweck der Übermittlung oder für die Markt- oder Meinungsforschung erfolgt.

Art. 37 Abs. 5 DS-GVO verlangt von dem Datenschutzbeauftragten, dass er beruflich hierzu qualifiziert ist und über ein entsprechendes Fachwissen verfügt. Sowohl die berufliche Qualifikation und als auch das hinreichende Fachwissen sind Benennungsvoraussetzungen für den Datenschutzbeauftragten.

Beide Qualifikationen müssen auf dem Gebiet des Datenschutzrechts sowie der Datenschutzpraxis bestehen und so ausgestaltet sein, dass der Datenschutzbeauftragte seine Pflichten aus Art. 39 DS-GVO erfüllen kann. Diese Pflichten liegen unter anderem in der Beratung des Verantwortlichen und der Beschäftigten. Sodann hat der nach Art. 39 Abs. 1 Buchst. b DS-GVO die Einhaltung der Verordnung und anderer Datenschutzvorschriften zu überwachen. Er bedarf deshalb neben des technischen Sachverstandes auch eingehender rechtlicher Kenntnisse.

Schließlich muss der Datenschutzbeauftragte nach Art. 39 Abs. 1 Buchst. d DS-GVO den Verantwortlichen im Zusammenhang der Datenschutz-Folgenabschätzung beraten. Wie bereits oben ausgeführt, kann sich diese Beratungsfunktion nicht nur auf die juristische oder technische Beratung beschränken. Der Datenschutzbeauftragte müsste jedenfalls auch in der Lage sein, Geschäftsprozesse so zu definieren oder zu modellieren, dass diese zum Gegenstand der Datenschutz-Folgenabschätzung gemacht werden können.

Über diese Pflichten hinaus sieht Art. 39 Abs. 1 Buchst. d und e DS-GVO vor, dass der Datenschutzbeauftragte als Ansprechpartner für die Aufsichtsbehörde zur Verfügung steht und für diese eine Anlaufstelle darstellt.

Die Stellung des Datenschutzbeauftragten ist in Art. 38 DS-GVO geregelt. Er ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Er hat, damit er seine Funktion ausüben kann, einen Anspruch auf Unterstützung sowie Zurverfügungstellung der erforderlichen Ressourcen. Zu diesen gehört auch ein Anspruch auf Zugang zu den personenbezogenen Daten und den entsprechenden Verarbeitungsvorgängen. Der Datenschutzbeauftragte ist eine Stabsstelle. Er berichtet unmittelbar an die oberste Managementebene (Art. 38 Abs. 3 Satz 3 DS-GVO).

Sein Fachwissen muss der Datenschutzbeauftragte laufend erhalten und aktualisieren. Sein Anspruch auf Unterstützung durch die verantwortliche Stelle erstreckt sich deshalb auch auf seine Fort- und Weiterbildung.

Der Datenschutzbeauftragte ist weisungsfrei und in seiner Funktion unabhängig. Er ist deshalb vor der Abberufung geschützt und ist in seiner Funktion nicht

zu benachteiligen. § 38 Abs. 2 BDSG i. V. m. § 6 Abs. 4 BDSG schützt den Datenschutzbeauftragten zudem vor einer Kündigung.

j) Internationaler Datenschutz

Die Übermittlung personenbezogener Daten innerhalb der Europäischen Union unterliegt den Regelungen der DS-GVO. Für diese Form der Datentransaktionen ist deshalb keine besondere über die DS-GVO hinausgehende Rechtslage zu beachten. Anders verhält es sich, wenn Daten in Drittländer exportiert werden.

Ein Datenexport stellt einen Verarbeitungsvorgang dar. Er ist deshalb nur dann rechtmäßig, wenn einer der Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO vorliegt. Zusätzlich zu den Rechtmäßigkeitsvoraussetzungen des Art. 6 Abs. 1 DS-GVO ist ein Datenexport nur möglich, wenn entweder ein Angemessenheitsbeschluss nach Art. 45 DS-GVO, geeignete Garantie nach Art. 46 DS-GVO oder Binding Corporate Rules (verbindliche interne Datenschutzvorschriften) nach Art. 47 DS-GVO vorliegen.

Art. 49 DS-GVO lässt unter sehr engen Voraussetzungen Ausnahmen von den drei Erlaubnistatbeständen (Angemessenheitsbeschluss, geeignete Garantien, Binding Corporate Rules) zu. Hierzu zählen beispielsweise die Einwilligung des Betroffenen oder die Erfüllung einer vertraglichen Verpflichtung zwischen dem Betroffenen und dem Verantwortlichen.

Die in Art. 46 DS-GVO genannten geeigneten Garantien dürften in der Datenschutzpraxis eine besondere Bedeutung erhalten. Solche geeigneten Garantien bedürfen grundsätzlich der Genehmigung der Aufsichtsbehörde. Allerdings sind Situationen in der DS-GVO geregelt, in denen auch ohne gesonderte Genehmigung der Aufsichtsbehörden solche Garantien als Grundlage für den Datenexport bzw. Datenverarbeitung im Drittland gemacht werden können. Zu diesen genehmigungsfreien Garantien gehören neben den rechtlich bindenden durchsetzbaren Dokumenten zwischen Behörden auch Binding Corporate Rules nach Art. 47 DS-GVO. Diese sind allerdings, wenn man Art. 47 DS-GVO einer genaueren Analyse unterzieht, ebenfalls auf der Grundlage einer Genehmigung durch die Aufsichtsbehörde gebildet.

In der Praxis bedeutsam dürften neben Zertifizierungen nach Art. 42 DS-GVO vor allen Dingen sog. EU-Standardvertragsklauseln **(Nr. 37–39)** oder von Aufsichtsbehörden angenommene Standarddatenschutzklauseln gehören. Soweit in der Vergangenheit bereits durch die EU-Kommission Standardvertragsklauseln beschlossen wurden, gelten diese auch unter der DS-GVO fort. Die EU-Kommission legte am 13. November 2020 Entwürfe zu aktualisierten Standardvertragsklauseln vor. Der Prozess der Abstimmung mit dem Europäischen Datenschutz-Ausschuss und dem Europäischen Datenschutzbeauftragten war zum Zeitpunkt des Redaktionsschlusses (15.April 2021) noch nicht abgeschlossen, sodass vom Abdruck der Standardvertragsklauseln abgesehen wurde.

Neben den Standardvertragsklauseln sind genehmigte Verhaltensregeln (Codes of Conduct) nach Art. 40 DS-GVO eine geeignete Grundlage, um beispielsweise im Rahmen einer internationalen Unternehmensgruppe zwischen den Gesellschaften Daten austauschen zu können. Die Artikel-29-Datenschutzgruppe hat Gestaltungshilfen veröffentlicht, die es Unternehmen ermöglichen sollen, ungeachtet der nach wie vor bestehenden unterschiedlichen Gesetzeslage in den Mitgliedstaaten der Europäischen Union sowie im Verhältnis zu Unter-

nehmen in Drittstaaten verbindliche unternehmensinterne Datenschutzregelungen zu schaffen. Damit wird im Sinne des „Selbstdatenschutzes" sowohl den unternehmensspezifischen Besonderheiten als auch der Vorstellung des Datenschutzes als qualitatives Merkmal des verarbeitenden Unternehmens Rechnung getragen.

k) Auftragsverarbeitung

Begriff des Auftragsverarbeiters. Auftragsdatenverarbeitung liegt nach Art. 4 Nr. 8 DS-GVO dann vor, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle im Auftrag des Verantwortlichen Daten verarbeitet. Der Auftragsdatenverarbeiter ist deshalb nicht gleichzusetzen mit dem Verantwortlichen selbst. Nach Art. 4 Nr. 7 DS-GVO ist dann von einem Verantwortlichen auszugehen, wenn dieser „alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung" entscheidet.

Der Auftragsverarbeiter ist also jener, der nicht über Zwecke bzw. Mittel der Auftragsverarbeitung entscheidet. Nach dem Working Paper 169 (WP 169)[1] der Artikel-29-Datenschutzgruppe ist dann davon auszugehen, dass kein Verantwortlicher vorliegt, wenn weder rechtlich noch tatsächlich Einfluss auf die Entscheidung, zu welchen Zwecken oder auf welcher Weise personenbezogene Daten verarbeitet werden, Einfluss genommen werden kann. Trifft eine Stelle alleine oder gemeinsam mit anderen allerdings eine Entscheidung über die Zwecke der Verarbeitung, ist diese stets als Verantwortlicher anzusehen.

Nach der Auffassung der Artikel-29-Datenschutzgruppe kann die Entscheidung über die Mittel durchaus auf den Auftragsverarbeiter delegiert werden. Dies bedeutet, dass ein Auftragsverarbeiter im Rahmen seines Auftrags zwar nicht darüber entscheiden kann, zu welchem Zweck die Verarbeitung erfolgt. Er könnte allerdings durchaus selbst darüber entscheiden, welche technischen Mittel eingesetzt werden, um diese Zwecke zu erreichen.

Zulässigkeit der Auftragsverarbeitung. Die DS-GVO enthält in Art. 28 und 29 Bedingungen, unter denen Auftragsverarbeitung zulässig ist. Art. 28 DS-GVO ist keine eigenständige Rechtsgrundlage, die neben Art. 6 Abs. 1 DS-GVO herangezogen werden könnte. Die Einbeziehung eines Auftragsverarbeiters ist nur im Rahmen des Art. 6 Abs. 1 DS-GVO möglich. Jedenfalls einer der dort genannten Tatbestände für eine rechtmäßige Verarbeitung personenbezogener Daten muss erfüllt sein, damit die Übermittlung personenbezogener Daten durch den Verantwortlichen an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter rechtmäßig sind.

Zwischen Verantwortlichem und Auftragsverarbeiter ist ein Vertrag über die Verarbeitung zu schließen. Dieser muss jedenfalls die in Art. 28 Abs. 3 DS-GVO genannten inhaltlichen Kriterien erfüllen. Der Vertrag ist schriftlich abzufassen. Dies kann allerdings auch „in einem elektronischen Format" erfolgen (Art. 28 Abs. 9 DS-GVO).

l) Gemeinsame Verantwortung

Legen zwei oder mehr Verantwortliche die Zwecke oder Mittel der Verarbeitung fest, so liegt keine Auftragsverarbeitung vor. Sie sind vielmehr gemein-

---

[1] Abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf.

sam Verantwortliche.[1] Die DS-GVO erlaubt eine solche Form der Zusammenarbeit in der Verarbeitung.

Beide Verantwortliche legen in einer speziellen Vereinbarung fest, wer von ihnen welche Verpflichtungen aus der DS-GVO erfüllt und diese insbesondere gegenüber dem Betroffenen wahrnimmt. So ist in einer solchen Vereinbarung insbesondere zu regeln, wer die Informationspflichten nach Art. 13 und 14 DS-GVO erfüllt.

m) Beschäftigtendatenschutz

Die DS-GVO sieht in Art. 88 vor, dass die Mitgliedstaaten von der Möglichkeit Gebrauch machen können, den Schutz der personenbezogenen Daten im Beschäftigungsverhältnis spezifisch zu regeln. Die Verordnung lässt dabei offen, ob diese Regelungen durch gesetzliche Bestimmungen oder durch Vereinbarungen der Tarifparteien erfolgen. Im Ergebnis ist deshalb auf der nationalen Ebene sowohl eine gesetzliche Ausgestaltung des Beschäftigtendatenschutzes als auch die Regelung des Datenschutzes im Rahmen von Betriebsvereinbarungen möglich.

Der Bundesgesetzgeber hat von dieser Möglichkeit jedenfalls teilweise Gebrauch gemacht. Mit § 26 BDSG ist eine Spezialvorschrift auf nationaler Ebene geschaffen worden, die sich mit der Wahrung des Datenschutzes im Beschäftigungsverhältnis befasst.

Demzufolge ist die Verarbeitung personenbezogener Daten zulässig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach der Begründung für dessen Durchführung oder Beendigung erforderlich ist. Ebenso ist die Verarbeitung personenbezogener Daten zulässig, wenn dies zur Ausübung oder Erfüllung gesetzlicher Pflichten oder eines Tarifvertrags, einer Dienst- oder Betriebsvereinbarung erforderlich ist.

Soll die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis auf eine Einwilligung gestützt werden, sind die strengen Anforderungen des § 26 Abs. 2 BDSG zu beachten und Wert darauf zu legen, dass die Freiwilligkeit der Einwilligung tatsächlich gegeben ist.

Die DS-GVO ihrerseits enthält in Art. 88 Abs. 2 spezifische Anforderungen an die inhaltliche Ausgestaltung von Betriebsvereinbarungen, die sich auch mit der Verarbeitung personenbezogener Daten befassen.

3. Das Bundesdatenschutzgesetz

Der Deutsche Bundestag verabschiedete am 27. April 2017 das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -umsetzungsgesetz EU – DSAnpUG-EU). Der Bundesrat stimmte dem Gesetz am 12. Mai 2017 zu.[2] Mit dem Gesetz erfolgt eine Neufassung des BDSG **(Nr. 6)**, die insgesamt aus vier Teilen besteht. Mit dem 2. Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU[3] nahm der Bundesge-

---

[1] Vgl. zur Verantwortlichkeit sowie deren Reichweite *EuGH*, Urt. v. 5.6.2018 – C-210/16 (Fanpage), ZD 2018, 357 m. Anm. *Marosi/Schulz* = MMR 2018, 591 m. Anm. *Moos/Rothkegel* sowie *EuGH*, Urt. v. 29.7.2019 – C-40/17 (FashionID), MMR 2019, 579 m. Anm. *Moos/Rothkegel*.

[2] BR-Drs. 332/17.

[3] BGBl. I 1626 vom 25.11.2019.

setzgeber im Jahr 2019 weitere Änderungen im BDSG vor, die vor allen Dingen die Benennungsschwelle des § 38 Abs. 1 Satz 1 BDSG für den Datenschutzbeauftragten betraf. Während zuvor diese Schwelle bei zehn Mitarbeitern lag, wurde diese auf zwanzig Mitarbeiter angehoben. An der allgemeinen Verpflichtung des Verantwortlichen zur Wahrung des Datenschutzes wurde durch diese gesetzgeberische Maßnahme nichts geändert.

Das BDSG enthält nun zunächst in den §§ 3 bis 21 gemeinsame Bestimmungen, die sowohl für öffentliche als auch nichtöffentliche Stellen gelten. In §§ 3 und 4 BDSG werden allgemeine Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen und für die Videoüberwachung geschaffen. Der Datenschutzbeauftragte öffentlicher Stellen wird in §§ 5 bis 7 BDSG verankert. Im Zuge der DS-GVO haben die Aufsichtsbehörden geänderte Aufgaben wahrzunehmen. Die Struktur der Aufsichtsbehörden sowie deren Aufgaben und Befugnisse werden folglich in §§ 8 bis 16 BDSG gesetzlich fixiert. Die Festlegung der deutschen Vertretung im Europäischen Datenschutzausschuss (§§ 17 bis 19 BDSG) sowie die Ausgestaltung der Rechtsbehelfe (§§ 20 und 21 BDSG) schließen den ersten Teil des BDSG ab.

Mit dem zweiten Teil des BDSG strebt der Gesetzgeber die Ausgestaltung der DS-GVO an.[1] Mit § 22 BDSG wird eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten geschaffen.[2] Die Zulässigkeitsvoraussetzungen für die Verarbeitungen zu anderen Zwecken durch öffentliche Stellen sowie durch nichtöffentliche Stellen und die Datenübermittlungen durch öffentliche Stellen werden in §§ 23 bis 25 BDSG gesetzlich verankert. Unter der Kapitelüberschrift der „Besonderen Verarbeitungssituationen" nimmt der Gesetzgeber Regelungen vor, die im Vorfeld des Gesetzgebungsvorhabens bereits Gegenstand intensiver Kritik waren: Beschäftigtendatenschutz (§ 26 BDSG),[3] Wissenschaftsprivileg (§ 27 BDSG),[4] Datenverarbeitung zu Archivzwecken (§ 28 BDSG),[5] Datenschutz bei Verbraucherkrediten (§ 30 BDSG) sowie dem Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften (§ 31 BDSG). Die Rechte des Betroffenen werden in §§ 32 bis 37 BDSG gefasst. Problematisch dürfte in diesem Zusammenhang sein, dass die Rechte des Betroffenen bereits im Rahmen der DS-GVO umfassend in Art. 12 bis 22 DS-GVO geregelt sind und lediglich im Rahmen des Art. 23 DS-GVO den Mitgliedstaaten in engen Grenzen die Möglichkeit zur Beschränkung der Betroffenenrechte eröffnet ist.[6] Inwieweit die nunmehr im BDSG enthaltenen Vorschriften europarechtlichen Bestand haben werden, bleibt abzuwarten. In der Praxis wird wohl zunächst die DS-GVO heranzuziehen sein. Für die Anwendung der Vorschriften des BDSG bleibt nur in den in der DS-GVO gesetzten eng umgrenzten Fällen Raum. Ergänzend zu den in der DS-GVO enthal-

---

[1] In diesem Zusammenhang sei auf die bereits an früherer Stelle erwähnten europarechtlichen Bedenken verwiesen.

[2] Siehe hierzu allerdings Art. 9 DS-GVO sowie *Schiff* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 9 Rn. 64.

[3] Siehe hierzu Art. 88 DS-GVO sowie *Selk* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 88 Rn. 69 ff.

[4] Siehe hierzu auch Art. 89 DS-GVO sowie *Raum* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 89 Rn. 52.

[5] Ebenda.

[6] Vgl. hierzu *Bertermann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 23 Rn. 3 ff.

tenen Bußgeldtatbeständen stellen §§ 41 und 43 BDSG zusätzliche Bußgeldtatbestände auf.

In seinem dritten Teil setzt das 1. DSAnpUG-EU die Vorgaben der Richtlinie EU 2016/680 um. Diese Vorschriften gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen. Neben den Regelungen zu den Rechtsgrundlagen der Verarbeitung, der Zweckbindung und der -änderung (§§ 47 bis 51 BDSG) werden die Betroffenenrechte mit den Regelungen der §§ 55 bis 61 BDSG ausgeformt. Der für die Verarbeitung Verantwortliche muss im Rahmen der Richtlinienumsetzung besondere Pflichten erfüllen. Diese beziehen sich sowohl auf die Situation der Auftragsdatenverarbeitung (§ 62 BDSG), der Datensicherheit und der Meldung von Datenschutzverletzungen (§§ 64 bis 66 BDSG), der Datenschutz-Folgenabschätzung, des Verarbeitungsverzeichnisses und der Protokollierung (§§ 67 bis 79 und 76 BDSG) als auch auf die Berichtigungs- und Löschungspflichten nach § 75 BDSG.

Im vierten Teil der BDSG-Novelle 2017 wendet sich der Gesetzgeber Datenverarbeitungen zu, die weder von der DS-GVO noch von der Richtlinie (EU) 2016/680 erfasst werden. Der Wortlaut des § 85 BDSG macht bereits deutlich, dass es sich hierbei um Ausnahmesituationen handelt, die v. a. auf Situationen der Verteidigung, der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich sind.

IV. Das Telemediengesetz

Das Telemediengesetz **(Nr. 8)** hat eine lange Geschichte. Im Jahre 1997 wurden mit dem Informations- und Kommunikationsdienstegesetz (IuKDG) rechtliche Rahmenbedingungen für die neuen Dienste in der Informationsgesellschaft, die Teledienste, geschaffen. Durch das Teledienstegesetz (TDG) entstanden Regeln für die Zulassungsfreiheit, die Informationspflichten und die Verantwortlichkeit für Inhalte. Die datenschutzrechtlichen Pflichten dieser Dienste wurden mit dem Teledienstedatenschutzgesetz (TDDSG) geregelt. Mit der europäischen „Richtlinie über den elektronischen Geschäftsverkehr" traten neue Regeln in Kraft, die in Deutschland mit dem „Elektronischen-Geschäftsverkehr-Gesetz" (EGG) im TDG umgesetzt wurden. Zugleich erfolgte eine Novellierung des TDDSG auf Grund der Erfahrungen und Entwicklungen seit Inkrafttreten des IuKDG. Bund und Länder haben sich Ende 2004 auf weitere Schritte verständigt, die Medienordnung zu entwickeln und am 19. April 2005 den „Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG)" vorgelegt. Das Bundeskabinett hat am 16. Juni 2006 den Entwurf für dieses Gesetz beschlossen. Am 18. Januar 2007 ist das Gesetz in dritter Lesung vom Bundestag verabschiedet worden. Es trat mit Wirkung zum 1. März 2007 in Kraft. Mit Art. 1 dieses Gesetzes wurden die rechtlichen Anforderungen für Tele- und Mediendienste in einem Telemediengesetz (TMG) zusammengefasst. Für das Thema des Datenschutzes sind der Geltungsbereich des Gesetzes (1.), das Anbieter-Nutzerverhältnis (2.), der Gesetzes- und Einwilligungsvorbehalt (3.), die organisatorischen Pflichten des Diensteanbieters (4.), der Schutz der Bestands- (5.) und

der Nutzungsdaten (6.) relevant. Mit dem am 19. November 2020 verabschiedeten jüngsten Änderungsgesetz, das am 27. November 2020 in Kraft trat, wurden vor allem Regelungen für audiovisuelle Mediendienste auf Abruf und Videosharingdienste geschaffen. Die Änderungen betreffen die im TMG bislang enthaltenen bereichsspezifischen Datenschutzvorschriften nur indirekt. Eine gesetzgeberische Anpassung des Teledienste-Datenschutzes steht noch aus. Der Entwurf eines Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) befindet sich aktuell im Beratungsablauf. Der Abdruck bleibt einer Folgeauflage vorbehalten.

Der EU-Gesetzgeber sah sich bei der Beratung und Verabschiedung der DS-GVO vor das Problem gestellt, dass für den speziellen Sektor der elektronischen Kommunikation mit der Richtlinie 2002/58/EG (ePrivacy-Richtlinie)[1] ein Regelungswerk bestand, das den Mitgliedstaaten aufgab, bereichsspezifische Datenschutzregelungen zu schaffen. Erwägungsgrund 173 der DS-GVO zeigt deutlich, dass dieser Regelungsbereich von der DS-GVO nicht erfasst und zugleich dem EU-Gesetzgeber die Aufgabe auferlegt werden sollte, eine Überarbeitung der ePrivacy-Richtlinie vorzunehmen. Diese Bemühungen sind bislang noch nicht abgeschlossen. Unter dem 10.1.2017 legte die EU-Kommission einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personen-bezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vor.[2] Das Europaparlament hat diesen Vorschlag beraten und empfohlen, im Rahmen des ordentlichen Gesetzgebungsverfahrens in den Trilog zwischen Kommission, Parlament und Rat einzutreten, um eine beschlussfähige Fassung des Verordnungsentwurfs beraten zu können. Dieser Prozess konnte nach langjährigen und intensiven Beratungen auf der Ebene der Mitgliedstaaten abgeschlossen werden. Am 10. Februar 2021 legte der Rat seinen Standpunkt zur geplanten ePrivacy-VO vor.[3] Bis zur Verabschiedung und dem Inkrafttreten einer ePrivacy-Verordnung gilt die bisherige Rechtslage in Gestalt der Datenschutzrichtlinie für elektronische Kommunikation (**Nr. 3**) weiter. Soweit in der Vergangenheit die Richtlinienvorgaben durch nationale Bestimmungen umgesetzt wurden, bleiben diese auch weiterhin anwendbar.

Zwar ist die ePrivacy-Verordnung als spezifische Regelung zur DS-GVO beabsichtigt, dies führt allerdings nicht dazu, dass im Bereich der elektronischen Kommunikation keine gesetzlichen Regelungen bestehen würden.

Mit Art. 95 DS-GVO wird deutlich gemacht, dass die DS-GVO den Verarbeitern dann keine zusätzlichen Pflichten auferlegt, wenn sie bereits bereichsspezifischen Vorschriften der elektronischen Kommunikation genügen müssen und soweit diese mit der DS-GVO vereinbar[4] sind.

---

[1] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. EG 2002 L 201, S. 37.

[2] EU-Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.1.2017, COM(2017) 10 final.

[3] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP, 2017/0003(COD) v. 10.2.2021.

[4] Art. 95 DS-GVO spricht davon, dass diese „dasselbe Ziel" verfolgen.

Im Ergebnis bedeutet dies, dass künftig die Bestimmungen der DS-GVO auch auf den Bereich der elektronischen Kommunikation anwendbar sind. Bestehende Regelungen sind dahingehend auszulegen, ob sie mit den Anforderungen der DS-GVO kompatibel sind. Ist dies der Fall, gelten die bisher auf nationaler Ebene in Umsetzung der ePrivacy-Richtlinie geschaffenen Bestimmungen weiter. Ist dies nicht der Fall, ist die DS-GVO zu beachten.[1)]

Für das Telemedienrecht haben die Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Rechtsauffassung entwickelt, dass die datenschutzrechtlichen Regelungen der §§ 11 ff. TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktreten. Dies hat Auswirkungen auf den Einsatz und die Nutzung spezifischer Web-Technologien. Die Datenschutzkonferenz der Aufsichtsbehörden vertritt deshalb die Auffassung, dass die §§ 12, 13 und 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung (z. B. Cookies) und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, nicht mehr angewendet werden können.[2)] Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann nur Art. 6 Abs. 1 DS-GVO[3)] herangezogen werden.

Die Orientierungshilfe der DSK gibt zwar die Rechtsauffassung der Aufsichtsbehörden wieder und lässt erwarten, auf welche Weise die Behörden datenschutzrechtlich die einschlägigen Sachverhalte behandeln werden. Vorbehaltlich einer höchstrichterlichen Entscheidung sowie einer europarechtlichen Stellungnahme zur Anwendbarkeit insbesondere des § 15 Abs. 3 TMG bleiben die Regelungen der §§ 11 ff. TMG für die Rechtsanwendung grundsätzlich in ihrer Geltung aber unverändert. Die Bestimmungen werden deshalb auch im Rahmen dieser Textsammlung abgedruckt.

Dem Rechtsanwender bleibt vor dem Hintergrund der geäußerten Auffassung der Aufsichtsbehörden nur die risikobezogene Abwägung, ob die Regelungen des TMG wie in der Vergangenheit auch angewendet werden sollen oder ob nicht vielmehr wegen des europarechtlich wohl geltenden Anwendungsvorrangs der DS-GVO die datenschutzrechtliche Gestaltung von Webseiten und der Einsatz spezifischer Tools (Cookies oder einschlägige Tracking- und Analysetools) an den Kriterien der DS-GVO gemessen werden müssen.

Rechtssicherheit werden letztlich nur eine möglicherweise künftig verabschiedete ePrivacy-Verordnung oder die Rechtsprechung des EuGH bringen können.

---

1) Vgl. zu dem komplexen Problem des Verhältnisses zwischen DS-GVO und den Bestimmungen der elektronischen Kommunikation *Klabunde/Selmayr* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 95 Rn. 1 ff.

2) Datenschutzkonferenz (DSK), Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Düsseldorf, 26.4.2018 sowie die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien vom 29.3.2019 der Datenschutzkonferenz, abzurufen unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf; vgl. hierzu auch *Gierschmann,* ZD 2018, 297; *Breyer,* ZD 2018, 302.

3) Dort vor allen Dingen die Tatbestände des Art. 6 Abs. 1 Buchst. a DS-GVO (Einwilligung), Art. 6 Abs. 1 Buchst. b DS-GVO (Erfüllung einer vertraglichen Verpflichtung gegenüber dem Betroffenen) sowie Art. 6 Abs. 1 Buchst. f DS-GVO (Vorliegen eines berechtigten Interesses, das nach einer Güterabwägung schwerer wiegt, als das Interesse des Betroffenen daran, dass die Verarbeitung unterbleibt).

Einführung

1. Geltungsbereich

Das Gesetz gilt nach § 1 Abs. 1 Satz 1 TMG für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG oder Rundfunk i. S. v. § 2 RStV sind.

Die zuvor in § 2 TDG und MDStV enthaltenen Regelbeispiele wurden zwar in die Regelung des TMG nicht aufgenommen, sind nach der Gesetzesbegründung aber weiterhin charakteristisch für Telemediendienste, wie

- Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit,
- Video auf Abruf, soweit es sich nicht nach Form und Inhalt um einen Fernsehdienst handelt,
- Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen,
- die kommerzielle Verbreitung von Informationen über Waren/Dienstleistungsangebote mit elektronischer Post.[1)]

Mit der Umsetzung der Richtlinie (EU) 2018/1808 vom 14. November 2018 und der dieser vorausgehenden Richtlinie 2010/13/EU (Richtlinie über audiovisuelle Mediendienste – AVMD-Richtlinie) wurde der Anwendungsbereich des Telemedienrechts auch auf diese Art der Mediendienste erstreckt und das Gesetz um spezifische Regelungen, insbesondere auch auf dem Gebiet der Informationspflichten und des Umgangs mit Nutzerbeschwerden ergänzt. In datenschutzrechtlicher Hinsicht wurde mit § 14a TMG eine Sondervorschrift gestaltet, mit der sichergestellt werden soll, dass personenbezogene Daten, die im Zusammenhang mit Altersverifikationssystemen verarbeitet werden, nicht zu kommerziellen Zwecken weiterverarbeitet werden.

Eine komplizierte Stellung zwischen TMG und TKG haben Telekommunikationsdienste, die neben der Übertragungsdienstleistung noch eine inhaltliche Dienstleistung anbieten, wie den Internetzugang und die E-Mail-Übertragung. Sie gelten wegen der Übertragungsdienstleistung als Telekommunikationsdienste und wegen der inhaltlichen Dienstleistung als Telemediendienste. Für sie gelten die Regeln des TMG zum Herkunftslandprinzip, zur Zugangsfreiheit und zur Haftungsprivilegierung. Der Datenschutz regelt sich nach dem TKG. Dies hat wesentliche Folgen für die E-Mail-Kommunikation: Die Telekommunikationsdiensteanbieter müssen das Fernmeldegeheimnis nach § 88 TKG beachten, Bestandsdaten (§ 95 TKG) und Verkehrsdaten (§ 96 TKG) speichern und die Sicherheitsbehörden können unter den gegebenen gesetzlichen Voraussetzungen auf diese Daten zugreifen (§§ 110 ff. TKG).[2)]

Die bisherigen Abgrenzungsschwierigkeiten, die in Folge einer allgemeinen Medienkonvergenz eher zunahmen, werden wohl erst mit einem zu erwartenden Telekommunikations-Telemedien-Datenschutz-Gesetz vermindert werden können. Insoweit bleibt auch vor dem Hintergrund einer erwarteten ePrivacy-Verordnung die weitere Rechtsentwicklung abzuwarten.

Für die Anwendung des TMG spielt es nach § 1 Abs. 1 Satz 2 keine Rolle, ob ein Diensteanbieter die Nutzung seiner Angebote ganz oder teilweise unentgeltlich oder gegen Entgelt ermöglicht.

[1)] BT-Drs. 16/3078, S. 13.
[2)] BT-Drs. 16/3078, S. 13.

In § 1 Abs. 1 Satz 2 TMG wird klargestellt, dass das Gesetz für private Anbieter und öffentliche Stellen gleichermaßen gilt. Es besteht kein Anlass, die öffentlichen Stellen aus dem Geltungsbereich des Gesetzes herauszunehmen, insbesondere nicht im Hinblick auf die Informationspflichten und die Haftungsprivilegierung.

2. Anbieter-Nutzer-Verhältnis

Die weit gefasste Begriffsbestimmung für Telemediendienste in § 1 Abs. 1 Satz 1 TMG erfordert für das Datenschutzrecht des TMG eine Klarstellung: Nach § 11 Abs. 1 TMG gelten die datenschutzrechtlichen Vorschriften nicht in Bereichen, in denen eine Anwendung der speziellen datenschutzrechtlichen Grundsätze des TMG als Schutzrecht für Endverbraucher nicht sachgerecht ist. Dies ist die Nutzung von Informations- und Kommunikationssystemen zu ausschließlich beruflichen oder dienstlichen Zwecken und zur ausschließlichen Steuerung von Arbeits- oder Geschäftsprozessen. Auch der Nutzerbegriff wurde durch § 11 Abs. 2 TMG anders als in § 2 Nr. 3 TMG geregelt, indem die juristischen Personen aus dem Nutzerbegriff herausgenommen wurden, da diese nicht Inhaber personenbezogener Daten sein können.[1] Mit § 11 Abs. 3 TMG werden die Datenschutzbestimmungen bei Telemediendiensten ergänzt, die zugleich dem Telekommunikationsdatenschutz unterliegen. Dies sind Anbieter für den Internetzugang und die E-Mail-Übertragung. Für diese Telemedienanbieter gelten die Datenschutzvorschriften des TKG und daneben nur bestimmte Datenschutzvorschriften des TMG: das Kopplungsverbot (§ 12 Abs. 3 TMG), die Möglichkeiten der Datenverarbeitung zur Bekämpfung von missbräuchlichen Nutzungen (§ 15 Abs. 8 TMG) und die dazugehörigen Sanktionen (§ 16 Abs. 2 Nr. 2 und 5 TMG).[2]

3. Gesetzes- und Einwilligungsvorbehalt[3]

§ 12 TMG regelt den Gesetzes- und Einwilligungsvorbehalt für das Erheben und Verwenden personenbezogener Daten. Personenbezogene Daten dürfen zur Bereitstellung von Telemedien nur erhoben und verwendet werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat (§ 12 Abs. 1 TMG).[4] Unter denselben Voraussetzungen ist die Verwendung personenbezogener Daten, die für die Bereitstellung von Telediensten erhoben worden sind, für andere Zwecke möglich (§ 12 Abs. 2 TMG). Die Bereitstellung von Telemedien darf der Diensteanbieter nicht von der Einwilligung des Nutzers in eine Verwendung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telemedien nicht oder in nicht zumutbarer Weise möglich ist. Die Vorschriften für den Schutz personenbezogener Daten sind auch anzuwenden, wenn die Daten nicht automatisiert verarbeitet werden (§ 12 Abs. 4 TMG).

---

[1] BT-Drs. 16/3078, S. 15.
[2] BT-Drs. 16/3078, S. 15 f.
[3] Auf die Rechtsauffassung der DSK vom 26.4.2018, wonach § 12 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktritt, wird in diesem Zusammenhang hingewiesen; a. A. *Gierschmann,* ZD 2018, 297; *Breyer,* ZD 2018, 302.
[4] BT-Drs. 16/3078, S. 16.

4. Organisatorische Pflichten des Diensteanbieters[1)]

Mit § 13 TMG werden die Pflichten des Diensteanbieters entsprechend § 4 TDDSG mit lediglich redaktionellen Änderungen übernommen. Es handelt sich um die Informationspflichten[2)] über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten (Abs. 1), um die Pflichten bei der elektronischen Einwilligung, die an den Wortlaut der im TKG entsprechend geregelten Vorschrift angepasst ist (Abs. 2 und 3),[3)] um die technischen und organisatorischen Vorkehrungen für den Datenschutz (Abs. 4), um die Anzeige der Weitervermittlung zu einem anderen Diensteanbieter (Abs. 5), die anonyme oder pseudonyme Zahlung (Abs. 6) und das Recht des Nutzers auf Auskunft (Abs. 7).

Folgt man der Rechtsauffassung der DSK, wonach § 13 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktritt, muss sich auch der Diensteanbieter mit den Anforderungen an ein wirksames Datenschutzmanagementsystem auseinandersetzen, wie es die DS-GVO intendiert. Dies gilt insbesondere auch hinsichtlich der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DS-GVO und die möglicherweise durchzuführende Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.

5. Bestandsdaten[4)]

a) Definition und der Grundsatz der Erforderlichkeit

Der Datenschutz der Bestandsdaten ist in § 14 TMG geregelt. Der Gesetzgeber hat in § 14 Abs. 1 TMG von einer katalogartigen Aufzählung möglicher Bestandsdaten abgesehen, weil die Vielfältigkeit möglicher Teledienste eine kasuistische Aufzählung ausschließt. Als typische Arten von personenbezogenen Daten, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Telemediendienste-Vertrages geeignet sind, gelten Name, Vorname, Anschrift, Rufnummer, Teilnehmer- oder Anschlusskennung, persönliches Kennwort, Passwort, E-Mail-Adresse, Geburtsdatum, Kreditkartennummer, Bankverbindung.[5)] Bestandsdaten können nach § 14 Abs. 1 TMG nur erhoben, verarbeitet und genutzt werden, wenn dies erforderlich ist. Das Kriterium der „Erforderlichkeit" ist für die Frage von erheblicher Bedeutung, ob ein Diensteanbieter im Vorfeld des Vertragsabschlusses Bestandsdaten über den Nutzer erheben darf. So verlangen Diensteanbieter häufig von Nutzern die Angabe personenbezogener Informationen, wenn der Nutzer das Angebot kostenlos sichten und Informationen auf seinen Rechner herunterladen will. Das TMG erlaubt durch § 14 Abs. 1 die Erhebung von Bestandsdaten nur zur Begründung, zur inhaltlichen

---

[1)] Auf die Rechtsauffassung der DSK vom 26.4.2018, wonach § 13 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktritt, wird in diesem Zusammenhang hingewiesen; a. A. *Gierschmann,* ZD 2018, 297; *Breyer,* ZD 2018, 302.

[2)] Vgl. zur Aufklärung des Betroffenen durch den Diensteanbieter *Helfrich* in: Hoeren/Sieber/Holznagel, Teil 16.1 Rn. 122 ff.

[3)] BT-Drs. 16/3078, S. 16.

[4)] Auf die Rechtsauffassung der DSK vom 26.4.2018, wonach wohl auch § 14 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktritt, wird in diesem Zusammenhang hingewiesen; a. A. *Gierschmann,* ZD 2018, 297; *Breyer,* ZD 2018, 302.

[5)] *Dix* in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDDSG Rn. 27–28.

Ausgestaltung oder Änderung eines Telemediendienste-Vertrages. Die Datenverarbeitung im Rahmen eines vorvertraglichen Vertrauensverhältnisses ist damit nicht erlaubt.[1] Die Pflicht zur Löschung von Bestandsdaten ist in § 14 TMG nicht ausdrücklich geregelt. Diese Pflicht ergibt sich aus dem Grundsatz der Erforderlichkeit. Nach diesem Grundsatz sind die Bestandsdaten zu löschen, wenn sie nicht mehr zur Begründung, Ausgestaltung und Änderung des Telemediendienste-Vertrags erforderlich sind, etwa weil das Vertragsverhältnis beendet ist und nachträgliche Ansprüche nicht mehr bestehen.

Folgt man der Rechtsauffassung der DSK, wonach wohl auch § 14 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktritt, muss sich der Diensteanbieter in Bezug auf die Rechtmäßigkeit der Verarbeitung von Bestandsdaten an den Anforderungen des Art. 6 Abs. 1 DS-GVO orientieren. Als mögliche Rechtsgrundlagen kommen neben einer Einwilligung nach Art. 6 Abs. 1 Buchst. a DS-GVO wohl Art. 6 Abs. 1 Buchst. b DS-GVO (Erfüllung einer vertraglichen Verpflichtung gegenüber dem Betroffenen) oder Art. 6 Abs. 1 Buchst. f DS-GVO (überwiegendes Interesse des Verarbeiters nach entsprechender Güterabwägung) in Betracht.

b) Das Recht zur Auskunft

§ 14 Abs. 2 TMG ergänzt die Befugnis zur Auskunftserteilung für Zwecke der Strafverfolgung, indem die Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst und der Militärische Abschirmdienst aufgenommen worden sind. Auf diese Weise wird der Kreis der Behörden, an die Bestandsdaten übermittelt werden dürfen, erweitert. Die Vorschrift konstituiert weder eine eigene Übermittlungsverpflichtung gegenüber den genannten Stellen, noch gibt sie diesen das Recht auf automatisierten Zugriff auf Kundendateien. Die Regelung soll lediglich klarstellen, dass die Anbieter von Telemediendiensten berechtigt sind, den genannten Stellen die Daten zu übermitteln, die diese berechtigt erheben und dass das Datenschutzrecht dies nicht verhindert. Damit wird klargestellt, dass Bestandsdaten aufgrund § 94 StPO beschlagnahmt werden dürfen und dass der Diensteanbieter die Daten gemäß § 95 StPO herauszugeben hat.[2]

Das Auskunftsrecht nach Art. 15 DS-GVO dürfte wohl in der Anwendung vorrangig sein. Die Einschränkung des Auskunftsanspruchs, wie er mit § 14 Abs. 2 TMG verbunden ist, könnte allerdings als eine zulässige Beschränkung der Betroffenenrechte nach Art. 23 Abs. 1 DS-GVO angesehen werden.

6. Nutzungsdaten[3]

§ 15 TMG regelt den Umgang mit Nutzungsdaten. Folgt man der Rechtsauffassung der DSK vom 26. April 2018 sowie der Orientierungshilfe vom 29. März 2019, wonach Art. 15 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurückzutreten hat, sind die nachstehenden Ausführungen zu

---

[1] *Dix* in: Roßnagel, Recht der Multimedia-Dienste, § 5 TDDSG Rn. 37–38.

[2] BT-Drs. 16/3078, S. 16.

[3] Folgt man der Rechtsauffassung der DSK, wonach § 15 TMG in der Anwendung hinter die Vorschriften der DS-GVO zurücktritt, muss die datenschutzrechtliche Verarbeitung von Nutzungsdaten den Voraussetzungen der DS-GVO genügen. Insbesondere sind die Anforderungen des Art. 6 Abs. 1 und Abs. 4 DS-GVO zu beachten.

Einführung

Inhalt und Reichweite des § 15 TMG entbehrlich.[1] Die jeweiligen Fallkonstellationen sind vor dem Hintergrund der DS-GVO zu beurteilen und die Rechtmäßigkeit dieser Verarbeitungen an den Kriterien des Art. 6 Abs. 1 DS-GVO zu messen. Dies gilt nicht zuletzt auch für die datenschutzrechtliche Zulässigkeit der Nutzung personenbezogener Daten zu Werbezwecken.

a) Definition

Nach der beispielhaften Auflistung in § 15 Abs. 1 TMG sind Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemediendienste. Hierzu gehören Steuerungsinformationen und Informationen zur Bestimmung der Interaktionspartner. Typische Steuerungsinformationen sind die Beschreibung des technischen Dienstes, der genutzt werden soll wie das File Transfer Protocol, die Bezeichnung einer Seite im World Wide Web als URL, die Anfragen bei einer Suchmaschine, Angaben über den eingesetzten Browsertyp, der mit Identifikationsdaten verbunden ist. Informationen zur Bestimmung des Interaktionspartners sind E-Mail-Adressen, Nutzerkennungen einschließlich persönlicher Identifikationsnummern (PIN) und Transaktionsnummern (TAN), IP-Adressen, die eine Identifikation des Nutzers, wie durch die statische Zuordnung, zulassen.

b) Zusammenführen von Nutzungsdaten zu Abrechnungszwecken

§ 15 Abs. 2 TMG stellt als Erlaubnistatbestand klar, dass Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemediendienste zusammengeführt werden dürfen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist. Die Vorschrift ist für die Anbieter von Online-Diensten von praktischer Relevanz, die den Zugang zu vielfältigen Telemediendiensten ermöglichen und für Access-Provider, die die technische Basis für den Zugang zum Internet bereitstellen. Nur wenn ein Anbieter die Abrechnung für verschiedene Telemediendienste übernimmt und für diesen Zweck die Zusammenführung von Nutzungsdaten verschiedener Anbieter erforderlich ist, dürfen diese Daten gemeinsam verarbeitet werden.[2] Außerhalb dieser Zweckbestimmung ist eine Zusammenführung nur unter den Voraussetzungen des § 12 Abs. 2 TMG zulässig. Danach darf der Diensteanbieter für die Durchführung von Telemediendiensten erhobene personenbezogene Daten für andere Zwecke nur verarbeiten und nutzen, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.[3]

c) Werbung

§ 15 Abs. 3 TMG enthält in Satz 1 die gesetzliche Erlaubnis des Diensteanbieters für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung von Pseudonymen zu erstellen.

---

[1] So auch *Nink* in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 15 TMG Rn. 1 ff.
[2] *Müller-Broich,* Telemediengesetz, 2012, § 15 Rn. 4 ff.
[3] BT-Drs. 14/6098, S. 29.

d) Abrechnungsdaten

Nach § 15 Abs. 4 TMG ist der Diensteanbieter berechtigt, Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus zu verarbeiten und zu nutzen, soweit sie für Zwecke der Abrechnung erforderlich sind. Sind Nutzungsdaten hierfür nicht erforderlich, so sind sie zu löschen. Zeitlicher Anknüpfungspunkt für die Löschung ist das Ende der jeweiligen Nutzung. Ist eine sofortige Löschung nicht oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so reicht die Löschung im Rahmen der täglichen Reorganisation des Datenbestandes aus.[1] Nach § 15 Abs. 4 Satz 2 TMG ist es möglich Daten zu sperren. Damit wird besonderen Aufbewahrungsfristen Rechnung getragen. So sind beispielsweise Bestands- und Abrechnungsdaten im Rahmen der kaufmännischen Buchführung nach Handelsrecht (§ 257 HGB, **Nr. 35**) und Steuerrecht (§ 147 AO, **Nr. 36**) zehn Jahre aufzubewahren, wenn sie Bestandteil kaufmännischer Belege sind.[2]

e) Übermittlung von Abrechnungsdaten

§ 15 Abs. 5 TMG regelt die Befugnisse des Diensteanbieters zur Übermittlung von Abrechnungsdaten an andere Diensteanbieter oder Dritte. Nach § 15 Abs. 5 Satz 1 TMG können Abrechnungsdaten an andere Diensteanbieter oder Dritte für Zwecke der Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer übermittelt werden. Nach § 15 Abs. 5 Satz 2 TMG darf der Diensteanbieter einem Dritten Abrechnungsdaten übermitteln, mit dem er einen Vertrag über den Einzug des Entgelts geschlossen hat und soweit es für diesen Zweck erforderlich ist. Damit ist das Outsourcing der Abrechnung von Telediensten erlaubt. Dieses Outsourcing ist mit einer ausdrücklichen Zweckbindung auf die Abrechnung beschränkt. Deshalb sind in dem Outsourcing-Vertrag die gesetzlichen Vorgaben möglichst konkret abzubilden.

f) Auskunft an die Strafverfolgungsbehörden

Nach § 15 Abs. 5 Satz 4 TMG hat der Diensteanbieter wie im Falle der Abrechnungsdaten (§ 14 Abs. 2 TMG) das Recht, den berechtigten Stellen Auskunft über die Nutzungsdaten zu erteilen, wenn die rechtlichen Voraussetzungen gegeben sind.

g) Inhalt der Abrechnung

§ 15 Abs. 6 TMG regelt den Detaillierungsgrad der Abrechnung von Telemediendiensten. Die Abrechnung darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit von einem Nutzer in Anspruch genommener Dienste nur erkennen lassen, wenn der Nutzer dies verlangt. Die Vorschrift ist eine Konkretisierung des Grundsatzes zur Datenvermeidung und Datenminimierung. Welche Angaben im Regelfall in einer Abrechnung erscheinen dürfen, richtet sich nach dem Abrechnungsmodus. Erscheint die Abrechnung als pauschaler nutzungsunabhängiger Betrag, als sog. Flatrate, so sind auf der Abrechnung keine Detailangaben zu vermerken. Nur wenn ein Nutzer einen Einzelnachweis verlangt, darf die Abrechnung auch Detailangaben über die in Anspruch genommenen Telemediendienste enthalten. Die Vorschrift bindet die Erstellung eines Einzel-

---

[1] *Schaar/Schulz* in: Roßnagel, Recht der Multimedia-Dienste, § 4 TDDSG Rn. 81.
[2] BT-Drs. 14/6098, S. 28.

nachweises daran, dass der Kunde einen solchen Nachweis verlangt. Der Begriff „Verlangen" ist für das Datenschutzrecht ungewöhnlich. Sinnvoll ist die Deutung, dass es sich um eine ausdrückliche Einwilligung handeln muss.

h) Löschungsfrist für Einzelnachweise

§ 15 Abs. 7 TMG passt die Löschungsfrist für Einzelnachweise an die Sechs-Monatsfrist bezüglich der Einzelnachweise in § 97 Abs. 3 TKG an. Abrechnungsdaten, für die ein Einzelnachweis verlangt wird, dürfen nach § 15 Abs. 7 Satz 1 TMG höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung gespeichert werden. Zu diesem Zeitpunkt sind die Abrechnungsdaten, für die ein Einzelnachweis verlangt wird, zu löschen. Über diesen Zeitpunkt hinaus dürfen sie nach § 15 Abs. 7 Satz 2 TMG nur im Ausnahmefall aufbewahrt werden, wenn innerhalb der Sechs-Monatsfrist Einwendungen gegen die Entgeltforderung erhoben worden sind oder diese trotz Zahlungsaufforderung nicht beglichen wurde.

i) Recht zur Datenverarbeitung bei Missbrauch von Telemediendiensten

§ 15 Abs. 8 TMG enthält einen Erlaubnistatbestand, der es einem Diensteanbieter ermöglicht, im Falle des Missbrauchs seiner Telemediendienste durch Nutzer deren Daten für Zwecke der Rechtsverfolgung zu verarbeiten, zu nutzen und an Dritte zu übermitteln. Die Regelung ist sachgerecht: Wie bei den Telekommunikationsanbietern dürfen die Datenschutzbestimmungen dem Diensteanbieter nicht die Möglichkeit nehmen, sich gegen schädigende Handlungen durch Nutzer zu wehren. Die Vorschrift ist eng gehalten. Insbesondere kann der Diensteanbieter nicht beliebig vorgehen. Er muss Anhaltspunkte, die die Annahme eines Missbrauchs durch einen Nutzer nahelegen, dokumentieren, damit diese gegebenenfalls von der Aufsichtsbehörde überprüft werden können.[1)]

j) Soziale Medien, Internet-Plattformen, Bewertungsportale und Datenschutz

Plattformen wie Facebook, Instagram, Twitter oder YouTube verändern die Kommunikation. Als Anbieter von Telemediendiensten unterliegen sie dem Telemediengesetz (TMG) und dessen datenschutzrechtlichen Anforderungen (§§ 11 bis 15 TMG). Diese Regeln gelten auch für Anbieter von Social-Community-Plattformen, die im nicht europäischen Ausland niedergelassen sind, wenn sie personenbezogene Daten im Inland erheben, Art. 3 Abs. 2 DS-GVO. Dies wird angenommen, wenn sich das Angebot äußerlich erkennbar an deutsche Nutzer richtet. So ist es üblich, dass Anbieter von Social-Network-Plattformen ihren Nutzern eine deutsche Eingabemaske unter einer .de-Domain bereitstellen und über Cookies deren Daten erfassen, die auf Rechnern im Inland gespeichert sind.

Nach der gesetzlichen Definition sind Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemediendienste, § 15 Abs. 1 Satz 2 Buchst. a) bis c)

[1)] BT-Drs. 14/6098, S. 30.

TMG. Es ist charakteristisch für Social-Community-Websites, dass die Nutzer persönliche Daten eingeben können wie Beziehungsstatus und Interessen. Diese Daten sind der wesentliche Inhalt der Social-Community-Websites. Es ist deshalb sinnvoll, diese Daten als Nutzungsdaten i. S. v. § 15 TMG zu bewerten und durch die Regeln des TMG zu schützen.[1)]

Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus nur für Zwecke der Abrechnung mit dem Nutzer verarbeiten und nutzen, § 15 Abs. 4 Satz 1 TMG. Eine weitere Datenverarbeitung, insbesondere für Zwecke der Werbung, ist nur aufgrund einer Einwilligung des Nutzers möglich, § 12 Abs. 2 TMG. Das TMG beschränkt sich darauf, die elektronische Einwilligung (§ 13 Abs. 2 TMG) zu regeln. Die übrigen Anforderungen an die Einwilligung ergeben sich aus Art. 4 Nr. 11 DS-GVO. Danach ist es wichtig, dass der Nutzer eines Telemediendienstes auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten hingewiesen wird.

Das datenschutzrechtliche Problem der Bewertungsportale für Lehrer und Professoren besteht in dem Konflikt zwischen dem Recht auf freie Meinungsäußerung und dem allgemeinen Persönlichkeitsrecht. Rechtliche Maßstäbe hat der Sechste Zivilsenat des Bundesgerichtshofs mit seinem „Spick-mich"-Urteil vom 23. Juni 2009 (VI ZR 196/08) entwickelt.[2)] Soweit in einem Bewertungsportal wahre Tatsachen und sachbezogene Wertungen mitgeteilt werden, ist dies zulässig. So stellte das Gericht für ein Lehrerbewertungsportal fest, dass als Tatsachen der Name des Lehrers und die unterrichteten Fächer genannt werden können und Bewertungen nach den Kriterien wie „guter/schlechter Unterricht", „fachlich kompetent/inkompent" durch das Recht auf freie Meinungsäußerung gedeckt sind und das allgemeine Persönlichkeitsrecht des bewerteten Lehrers nicht verletzen.

V. Weitere datenschutzrechtliche Regeln

Das Grundgesetz **(Nr. 15)** gewährt Datenschutz durch das aus Art. 1 und 2 GG abgeleitete informationelle Selbstbestimmungsrecht und das Fernmeldegeheimnis des Art. 10 GG. Dies strahlt auf das Gesetz zu Art. 10 GG **(Nr. 16),** auf Regeln des Strafgesetzbuches **(Nr. 20)** und der Strafprozessordnung **(Nr. 19)** aus. Im öffentlichen Dienst besteht Datenschutz durch das Beamtenstatusgesetz[3)] und das Bundesbeamtengesetz **(Nr. 21),** im Arbeitsrecht durch das Betriebsverfassungsgesetz **(Nr. 22).** Sozialdatenschutz ist ein aufgefächertes Thema: Datenschutz besteht für die Fälle der Arbeitssuche, der Sozialversicherung, der Krankenversicherung, der Rentenversicherung, der Unfallversicherung, der Jugendhilfe, der Rehabilitation, des Sozialverwaltungsverfahrens, der Sozialpflegeversicherung und der Sozialhilfe **(Nr. 23–34).** Für den Datenschutz im Wirtschaftsverkehr hat die EU-Kommission Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer entwickelt **(Nr. 37–39).** In das Aufgabengebiet des Datenschutzbeauftragten des Bundes

---

[1)] Siehe zu dieser Diskussion *Bauer,* MMR 2008, 435 (436).

[2)] MMR 2009, 608 m. Anm. *Greve/Schärdel;* zu den Urteilen der Vorinstanz siehe *Greve/Schärdel,* MMR 2008, 644 (645); vgl. ferner zu Ärztebewertung *BGH,* ZD 2016, 281 m. Anm. *Palzer; BGH,* ZD 2015, 85 m. Anm. *Petershagen* und *BGH,* MMR 2014, 704 m. Anm. *Palzer* sowie *OLG Dresden,* GRUR-Prax 2018, 217 und *BGH,* Urt. v. 20.2.2018 – VI ZR 30/17; zu Hotelbewertungen *BGH,* MMR 2015, 726 m. Anm. *Milstein.*

[3)] Vom Abdruck wurde abgesehen.

fällt das Informationsfreiheitsgesetz **(Nr. 7).** Dieses Gesetz gibt jedem gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen. Der Anspruch ist durch umfangreiche Ausnahmen gekennzeichnet, wie mögliche nachteilige Auswirkungen auf internationale Beziehungen und die Gefährdung der öffentlichen Sicherheit.

Im Zusammenhang mit der Wirksamkeit der DS-GVO traten vermehrt Unsicherheiten und Zweifel auf, ob und inwieweit durch die europarechtliche Regelung bestehende nationale Vorschriften zum Schutz der Persönlichkeitsrechte verdrängt werden. So musste die Frage geklärt werden, ob und in wieweit die Vorschriften der DS-GVO für Fotografen vordringlich zu beachten sind. Das OLG Köln setzte sich in einem Beschluss vom 18.6.2018 mit dieser Abgrenzungsfrage auseinander und betonte, dass die insoweit einschlägige Vorschrift des § 23 KUG von der DS-GVO nicht verdrängt werde.[1] Da die Diskussion um die Reichweite des Art. 85 DS-GVO wohl mit dieser Entscheidung noch nicht abgeschlossen sein dürfte, wurde das KUG **(Nr. 13)** mit einem Auszug in diese Textsammlung aufgenommen.

Die Nutzung personenbezogener Daten zu werblichen Zwecken muss mit dem Wirksamwerden der DS-GVO den darin fixierten gesetzlichen Vorgaben folgen. Wie bereits die ersten Wochen nach dem 25.5.2018 zeigten, warfen die Anforderungen an die Rechtmäßigkeit einer Verarbeitung allerdings nicht nur Fragen des Art. 6 Abs. 1 DS-GVO auf. Die werbliche Nutzung personenbezogener Daten hat ebenso den Anforderungen des Wettbewerbsrechts und insbesondere § 7 UWG zu folgen. Um dem praktischen Bedürfnis der regelungstechnischen Abgrenzung beider Rechtsgebiete Rechnung tragen zu können, wurde das UWG mit einem Auszug ebenfalls in diese Textsammlung aufgenommen **(Nr. 11)**.

Zwar handelt es sich bei den Regelungen des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) (**Nr. 12**) streng genommen nicht um datenschutzrechtliche Vorschriften. Der Anwendungsbereich überschneidet sich jedoch in bestimmten Sachverhalten durchaus mit demjenigen der DS-GVO. Das GeschGehG wurde im Interesse einer Abgrenzung in der datenschutzrechtlichen Praxis in die Textsammlung ebenfalls aufgenommen.

Schließlich ist auf das Unterlassungsklagengesetz (UKlaG) **(Nr. 14)** hinzuweisen, das unter bestimmten Voraussetzungen auch auf datenschutzrechtliche Verletzungshandlungen anwendbar ist.

Die im Rahmen der Erfüllung von Löschungspflichten aus Art. 17 DS-GVO zu beachtenden handels- oder steuerrechtlichen Aufbewahrungspflichten führten zu einer Aufnahme der insoweit einschlägigen Vorschriften des HGB **(Nr. 35)** und der AO **(Nr. 36)**.

VI. Ausblick

Cloud, Social Media, mobile Kommunikation sowie eMobility, Smart Home oder auch Smart City sind die Merkmale einer ständig wachsenden Netzgesellschaft. Nutzer jeder Art, von Großunternehmen bis zu Einzelnutzern speichern ihre Daten in der Cloud und rufen sie mit mobilen Kommunikationsmitteln von beliebigen Orten wieder ab. Social-Media-Dienste werden genutzt, um Daten an einen stetig wachsenden Kreis von Freunden zu verteilen.

[1] *OLG Köln*, ZD 2018, 434 m. Anm. *Hoeren*.

Diese Entwicklung ist eine Herausforderung für den Datenschutz.[1] Die Internationalisierung der Datenspeicherung und der Kommunikation macht die Wirkung national begrenzter Datenschutzgesetzgebung fragwürdig. Der Zuspruch, den Social-Media-Dienste finden, die Daten verteilen, berührt die Idee des Datenschutzes in seiner Grundlage. Ebenso stellt der mögliche Missbrauch personenbezogener Daten zu Zwecken der Beeinflussung von Wählerverhalten, wie dies im Fall Facebook/Cambridge Analytica[2] vermutet wird, den Datenschutz vor neue Herausforderungen, die weit über den Schutz des Einzelnen hinausgehen und das gesellschaftliche Verständnis des Datenumgangs berühren.

In diese Bewährungsphase des Datenschutzes fällt die Verabschiedung der Datenschutz-Grundverordnung **(Nr. 1)** sowie der JI-Richtlinie **(Nr. 2).** Mit der Verordnung wird für sämtliche Mitgliedstaaten ein einheitlicher datenschutzrechtlicher Rahmen geschaffen. Anders als bei Richtlinien haben die Mitgliedstaaten bei Verordnungen keinen Handlungsspielraum. Verordnungen haben nach Art. 288 Abs. 2 AEUV unmittelbare Wirkung und bedürfen deshalb keines nationalen Umsetzungsakts. Dies hat erhebliche Rechtsfolgen für die Mitgliedstaaten. Soweit die EU-Verordnung datenschutzrechtliche Sachverhalte regelt, besteht kein Raum mehr für ein entsprechendes deutsches Datenschutzrecht. Es gilt direkt die Grundverordnung, für deren Auslegung der EuGH im Vorabentscheidungsverfahren (Art. 267 Abs. 1 Buchst. b AEUV) zuständig ist. Die Verordnung enthält eine Vielzahl an Klauseln, die den Mitgliedstaaten die Aufrechterhaltung oder die Schaffung spezifischerer Datenschutzregelungen gestatten, um so die in der Grundverordnung festgelegten datenschutzrechtlichen Rahmenbedingungen zu spezifizieren. Vor diesem Hintergrund stehen vielfältige gesetzgeberische Herausforderungen auf Bundes- oder auch auf Landesebene bevor, da der Gesetzgeber das nationale Datenschutzrecht verordnungskonform um- und auszugestalten hat.[3]

Die Verordnung macht in vielerlei Hinsicht eine Anpassung bestehender Prozesse auf Seiten der mit der Verarbeitung personenbezogener Daten befassten Unternehmen erforderlich. Die Umsetzung der Anforderungen der DS-GVO kann dabei durchaus nicht aufgeschoben werden. Bußgelder können ab Inkrafttreten der DS-GVO bis zu 4 Prozent des Weltumsatzes eines Unternehmens betragen. Gleichzeitig verschärfen sich die Haftungsszenarien für die Unternehmensleitung.[4]

Eine Analyse der DS-GVO zeigt, dass unabhängig von den zu erwartenden Anpassungen des nationalen Rechts bereits kurzfristig auf folgenden Gebieten Gestaltungsbedarf besteht:

– Anpassung der Anforderungen an eine datenschutzrechtlich wirksame Einwilligung an die technische Entwicklung,
– umfassende Informations- und Dokumentationspflichten, um eine Transparenz der Verarbeitungsverfahren herzustellen,

---

[1] Hierzu *Forgó* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, I. 2.

[2] *Selmayr,* ZD 2018, 197.

[3] Vgl. hierzu die Webseiten der Datenaufsichtsbehörden der Länder sowie der Datenschutzkonferenz. Hier finden sich eine Vielzahl von konkreten Handlungsempfehlungen. Auf den Internetauftritt der DSK unter www.datenschutz-konferenz.de wird ausdrücklich hingewiesen. Dort sind neben Kurzpapieren vor allen Dingen Orientierungshilfen zu finden, die für die datenschutzrechtliche Praxis von außerordentlich großer Bedeutung sind und laufend aktualisiert werden.

[4] Eine eindrückliche Dokumentation der in Anwendung der DS-GVO in den EU-Mitgliedstaaten ausgelösten Bußgeldverfahren ist unter www.enforcementtracker.com zu finden.

– erweiterte Auskunfts- und Betroffenenrechte,
– Anpassung bestehender Speicher- und Löschkonzepte zur Erfüllung des „Rechts auf Vergessenwerden“,
– Erfüllung des Anspruchs auf Datenportabilität,
– Einführung eines Systems der Datenschutz-Folgenabschätzung (Risikoanalyse),
– Erweiterung der Haftung bei Auftragsdatenverarbeitung,
– mögliche Neuinterpretation des Beschäftigtendatenschutzes vor dem Hintergrund der DS-GVO,
- Annäherung des Datenschutzes an die Compliance im Unternehmen, indem der Aspekt der Prävention betont wird,
– Stärkung des betrieblichen Datenschutzbeauftragten, in dem diesem eine explizite Überwachungspflicht auferlegt und das Unternehmen verpflichtet wird, ihn so früh wie möglich in Geschäftsprozesse einzubeziehen.

Für die Erfüllung der datenschutzrechtlichen Anforderungen der DS-GVO bestehen neben dem in Art. 83 DS-GVO angelegten Bußgeldrisiko gewichtige kaufmännische Gründe: Die Rechtsprechung hat in der jüngsten Vergangenheit wiederholt die Verletzung datenschutzrechtlicher Vorschriften als wettbewerbswidriges Verhalten gewertet und hieran Unterlassungsansprüche geknüpft.[1] Damit wird die Einhaltung datenschutzrechtlicher Vorschriften nicht zuletzt im Wettbewerb konkurrierender Unternehmen zu einem Faktor des kaufmännischen Erfolges: Wird die Nutzung eines Datenbestandes beispielsweise deshalb untersagt, weil die Datenportabilität nicht sichergestellt werden kann, droht dem Unternehmen, das sein Vertriebskonzept auf personenbezogenen Daten gründet, ein erheblicher Schaden, der neben dem Reputationsschaden nur langsam wieder kompensiert werden kann. Ob die Anwendung wettbewerbsrechtlicher Vorschriften auf Datenschutzverstöße nach dem Inkrafttreten der DS-GVO in Betracht kommen kann, ist umstritten. Die wohl herrschende Meinung geht davon aus, dass die DS-GVO die Verfolgung von Verletzungshandlungen abschließend regelt und folglich für die Anwendung wettbewerbsrechtlicher Regelungen kein Raum verbleibt.[2]

Sofern ein datenschutzrechtlicher Sachverhalt grenzüberschreitende und damit europäische Wirkung entfaltet, hat das nationale Gericht den ihm unterbreiteten Sachverhalt im Hinblick auf die Auslegung der DS-GVO dem EuGH vorzulegen. Dieser prüft dann nicht zuletzt auch vor dem Hintergrund der Europäischen Grundrechtecharta sowie des im AEUV enthaltenen Primärrechts die betreffende Vorschrift der Verordnung auf ihre grundrechtliche Ausgestaltung. Nationales Datenschutzrecht sowie die hierzu ergangene Rechtsprechung des BVerfG werden nicht per se obsolet, auch wenn dies im Rahmen der Diskussion um die Ausgestaltung der DS-GVO vereinzelt befürchtet wurde. Soweit die Grundverordnung durch nationales Recht ausgestaltet wird bzw. das europäische Recht nicht einschlägig ist oder auch im öffentlichen Bereich nach wie vor der nationale Gesetzgeber originär kompetent ist, sind die bestehenden Ent-

---

[1] *LG Düsseldorf*, ZD 2016, 231; *OLG Karlsruhe*, ZD 2012, 432; *LG Würzburg*, ZD 2019, 38 m. Anm. *Schlüter*; a. A. *OLG München*, MMR 2012, 317 m. Anm. *Schröder; OLG Düsseldorf*, MMR 2017, 254 m. Anm. *Meyer; LG Berlin*, MMR 2018, 328 m. Anm. *Heldt*. Kritisch zum wettbewerbsrechtlichen Unterlassungsanspruch bei Datenschutzverletzungen *Baumgartner/Sitte*, ZD 2018, 555; *Wolf*, ZD 2018, 248; *Ohly*, GRUR 2019, 686.

[2] Vgl. *Ohly*, GRUR 2019, 686; *Köhler* in: Köhler/Bornkamm, UWG, 38. Aufl. 2020, § 3a Rn. 1.40a, der sich insbesondere auch mit der jüngeren Rechtsprechung des EuGH in diesem Zusammenhang auseinander setzt.

scheidungen des Bundesverfassungsgerichts heranzuziehen. Ein ausgesprochenes Ziel der DS-GVO ist die Anpassung des Datenschutzrechts an die technischen Innovationen, die mit dem Internet seit Verabschiedung der DS-RL im Jahre 1995 eingetreten sind.

Im Ergebnis befindet sich das Datenschutzrecht in einer Umbruchphase. Es wird sich in den nächsten Jahren zeigen, in wieweit die Idee des Datenschutzes den neuen Formen der Kommunikation, die durch Mobilität der Nutzer und Internationalisierung der Anbieter gekennzeichnet ist, sowie der immer intensiveren Integration und Vernetzung der Lebens- und Wirtschaftsbereiche so Rechnung tragen kann, dass ein Ausgleich zwischen dem Schutz des Persönlichkeitsrechts des Einzelnen und den wirtschaftlichen Interessen der Unternehmen sowie der gesellschaftlichen Entwicklung erzielt werden kann.

VII. Synopse der Erwägungsgründe und Artikel der DS-GVO

Die DS-GVO ist nach Art. 288 Abs. 2 AEUV in allen ihren Teilen verbindlich. Die Erwägungsgründe gehören jedoch nicht zum verfügenden Teil der Verordnung und sind als solche nicht rechtsverbindlich.[1] Den Erwägungsgründen kommt allerdings für die Auslegung[2] der Verordnung eine zentrale Bedeutung zu, da sie oftmals Ausdruck des politischen Kompromisses sind, wie er im Gesetzgebungsverfahren sowohl im Rahmen der parlamentarischen als auch der Behandlung im Rat letztlich zum verabschiedeten Rechtsakt führte.[3] Um die Arbeit mit der DS-GVO in der Praxis für die Rezeption der Erwägungsgründe zu öffnen, sind den Bestimmungen der DS-GVO die einzelnen Erwägungsgründe wie folgt zuzuordnen:

Bestimmungen der VO (EU) 2016/679	**Erwägungsgründe zu VO (EU) 2016/679**
Kapitel I Allgemeine Bestimmungen	EG 1–37
Artikel 1	EG 1–13
Artikel 2	EG 14–21
Artikel 3	EG 22–25
Artikel 4	EG 26–37
Kapitel II Grundsätze	EG 38–57
Artikel 5	EG 39
Artikel 6	EG 32, 40–50, 55, 56
Artikel 7	EG 32, 33, 42, 43
Artikel 8	EG 38
Artikel 9	EG 51–56

[1] So mit eingehendem Nachweis auf die Rechtsprechung des EuGH *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 97.

[2] Zu der Bedeutung der außerhalb des Rechtsakts stehenden Dokumente für die Auslegung nahm der EuGH in seiner Entscheidung vom 26.2.1991, in welcher er verlangt, dass die Quelle in der fraglichen Bestimmung des Rechtsaktes ihren Ausdruck gefunden hat. *EuGH*, Urt. v. 26.2.1991 – C-292/89 (The Queen/Immigration Appeal Tribunal, ex parte Antonissen), BeckEuRS 1991, 176674 = BeckRS 2004, 76058, Rn. 18.

[3] *Selmayr/Ehmann* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Einführung Rn. 97.

Bestimmungen der VO (EU) 2016/679	Erwägungsgründe zu VO (EU) 2016/679
Artikel 10	
Artikel 11	EG 57
Kapitel III Rechte der betroffenen Person	EG 58–73
Abschnitt 1 Transparenz und Modalitäten	
Artikel 12	EG 58, 59
Abschnitt 2 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten	
Artikel 13	EG 60–62
Artikel 14	EG 61, 62
Artikel 15	EG 63, 64
Abschnitt 3 Berichtigung und Löschung	
Artikel 16	EG 65
Artikel 17	EG 65
Artikel 18	EG 67
Artikel 19	
Artikel 20	EG 68
Abschnitt 4 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall	
Artikel 21	EG 69, 70
Artikel 22	EG 71, 72
Abschnitt 5 Beschränkungen	
Artikel 23	EG 73
Kapitel IV Verantwortlicher und Auftragsverarbeiter	EG 74–100
Abschnitt 1 Allgemeine Pflichten	
Artikel 24	EG 74–77
Artikel 25	EG 78
Artikel 26	EG 79
Artikel 27	EG 80
Artikel 28	EG 81
Artikel 29	
Artikel 30	EG 82
Artikel 31	
Abschnitt 2 Sicherheit personenbezogener Daten	
Artikel 32	EG 83
Artikel 33	EG 85, 87, 88
Artikel 34	EG 86

Bestimmungen der VO (EU) 2016/679	Erwägungsgründe zu VO (EU) 2016/679
Abschnitt 3 Datenschutz-Folgenabschätzung und vorherige Konsultation	
Artikel 35	EG 84, 89–93
Artikel 36	EG 94–96
Abschnitt 4 Datenschutzbeauftragter	
Artikel 37	EG 97
Artikel 38	
Artikel 39	
Abschnitt 5 Verhaltensregeln und Zertifizierung	
Artikel 40	EG 98, 99
Artikel 41	
Artikel 42	EG 100
Artikel 43	
Kapitel V Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen	EG 101–116
Artikel 44	
Artikel 45	EG 101–107
Artikel 46	EG 108, 109
Artikel 47	EG 110
Artikel 48	EG 115
Artikel 49	EG 111–114
Artikel 50	EG 116
Kapitel VI Unabhängige Aufsichtsbehörden	EG 117–129
Abschnitt 1 Unabhängigkeit	
Artikel 51	EG 117, 119
Artikel 52	EG 118, 120
Artikel 53	EG 121
Artikel 54	
Abschnitt 1 Zuständigkeit, Aufgaben und Befugnisse	
Artikel 55	EG 122, 123
Artikel 56	EG 124–128
Artikel 57	EG 123, 132
Artikel 58	EG 129
Artikel 59	
Kapitel VII Zusammenarbeit und Kohärenz	EG 130–140
Abschnitt 1 Zusammenarbeit	
Artikel 60	EG 130, 131
Artikel 61	EG 133

Bestimmungen der VO (EU) 2016/679	Erwägungsgründe zu VO (EU) 2016/679
Artikel 62	EG 133, 134
Abschnitt 2 Kohärenz	
Artikel 63	EG 135, 136
Artikel 64	EG 136
Artikel 65	
Artikel 66	EG 137, 138
Artikel 67	
Abschnitt 3 Europäischer Datenschutz-ausschuss	
Artikel 68	EG 139
Artikel 69	
Artikel 70	
Artikel 71	
Artikel 72	
Artikel 73	
Artikel 74	
Artikel 75	EG 140
Artikel 76	
Kapitel VIII Rechtsbehelfe, Haftung, Sanktionen	EG 141–152
Artikel 77	EG 141, 142
Artikel 78	EG 143, 144
Artikel 79	EG 145
Artikel 80	EG 142
Artikel 81	EG 144, 145
Artikel 82	EG 146, 147
Artikel 83	EG 148, 150, 151
Artikel 84	EG 149, 152
Kapitel IX Vorschriften für besondere Verarbeitungssituationen	EG 153–165
Artikel 85	EG 153–165
Artikel 86	EG 154
Artikel 87	
Artikel 88	EG 155
Artikel 89	EG 156–163
Artikel 90	EG 164
Artikel 91	EG 165
Kapitel X Delegierte Rechtsakte und Durchführungsrechtsakte	EG 166–170
Artikel 92	EG 166–169
Artikel 93	EG 170
Kapitel XI Schlussbestimmungen	EG 171–173
Artikel 94	EG 171–173

Bestimmungen der VO (EU) 2016/679	Erwägungsgründe zu VO (EU) 2016/679
Artikel 95	EG 173
Artikel 96	
Artikel 97	
Artikel 98	
Artikel 99	EG 171

VIII. Synopse der Artikel der DS-GVO und des BDSG

Der Bundesgesetzgeber hat von der Möglichkeit Gebrauch gemacht, mit spezifizierenden Regelungen Gestaltungsspielräume auszuschöpfen, die von der DS-GVO eingeräumt werden. Im Einzelfall kann deshalb für die Rechtsanwendung eine Gegenüberstellung jener Vorschriften des BDSG hilfreich sein, die direkt oder indirekt auf die DS-GVO Bezug nehmen. Mit der nachstehenden Synopse soll diesem Informationsbedürfnis Rechnung getragen werden. Gleichzeitig ist darauf hinzuweisen, dass durchaus im Einzelfall der europarechtliche Anwendungsvorrang der DS-GVO auch dann zu beachten sein kann, wenn auf nationaler Ebene eine Vorschrift besteht, die mit Regelungen der DS-GVO korrespondiert und die Berufung des nationalen Gesetzgebers auf eine Spezifizierungsklausel jedenfalls fraglich ist.[1)]

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
Kapitel I Allgemeine Bestimmungen	
Artikel 1	
Artikel 2	§ 1 Anwendungsbereich des Gesetzes
Artikel 3	§ 1 Abs. 4 Anwendungsbereich des Gesetzes
Artikel 4	§ 2 Begriffsbestimmungen
	§ 26 Abs. 8 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
Kapitel II Grundsätze	
Artikel 5	
Artikel 6	§ 3 Verarbeitung personenbezogener Daten durch öffentliche Stellen
	§ 4 Videoüberwachung öffentlich zugänglicher Räume
	§ 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen

1) Siehe hierzu *Franck*, ZD 2018, 345.

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
	§ 24 Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen
	§ 25 Datenübermittlungen durch öffentliche Stellen
Artikel 7	
Artikel 8	
Artikel 9	§ 22 Verarbeitung besonderer Kategorien personenbezogener Daten
	§ 24 Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen
	§ 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statischen Zwecken
	§ 28 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken
Artikel 10	
Artikel 11	
Kapitel III Rechte der betroffenen Person	
Abschnitt 1 Transparenz und Modalitäten	
Artikel 12	
Abschnitt 2 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten	
Artikel 13	§ 29 Abs. 2 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten
	§ 32 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
Artikel 14	§ 29 Abs. 1 Satz 1 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
	§ 32 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
Artikel 15	§ 29 Abs. 1 Satz 2 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten
	§ 30 Verbraucherkredite
	§ 34 Auskunftsrecht der betroffenen Person
Abschnitt 3 Berichtigung und Löschung	
Artikel 16	
Artikel 17	§ 35 Abs. 1 und 3 Recht auf Löschung
Artikel 18	§ 35 Abs. 2 Recht auf Löschung
Artikel 19	
Artikel 20	
Abschnitt 4 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall	
Artikel 21	§ 36 Widerspruchsrecht
Artikel 22	§ 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften
	§ 37 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
Abschnitt 5 Beschränkungen	
Artikel 23	
Kapitel IV Verantwortlicher und Auftragsverarbeiter	
Abschnitt 1 Allgemeine Pflichten	
Artikel 24	
Artikel 25	
Artikel 26	
Artikel 27	
Artikel 28	
Artikel 29	
Artikel 30	
Artikel 31	
Abschnitt 2 Sicherheit personenbezogener Daten	
Artikel 32	

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
Artikel 33	
Artikel 34	§ 29 Abs. 1 Satz 3 und 4 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten
Abschnitt 3 Datenschutz-Folgenabschätzung und vorherige Konsultation	
Artikel 35	
Artikel 36	
Abschnitt 4 Datenschutzbeauftragter	
Artikel 37	§ 5 Benennung
	§ 38 Abs. 1 Datenschutzbeauftragte nichtöffentlicher Stellen
Artikel 38	§ 6 Stellung
	§ 38 Abs. 2 Datenschutzbeauftragte nichtöffentlicher Stellen
Artikel 39	§ 7 Aufgaben
Abschnitt 5 Verhaltensregeln und Zertifizierung	
Artikel 40	
Artikel 41	
Artikel 42	
Artikel 43	§ 39 Akkreditierung
Kapitel V Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen	
Artikel 44	
Artikel 45	
Artikel 46	
Artikel 47	
Artikel 48	
Artikel 49	
Artikel 50	
Kapitel VI Unabhängige Aufsichtsbehörden	
Abschnitt 1 Unabhängigkeit	
Artikel 51	§ 8 Errichtung
	§ 9 Zuständigkeit
	§ 17 Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
	§ 18 Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder
	§ 40 Aufsichtsbehörden der Länder
Artikel 52	§ 10 Unabhängigkeit
	§ 13 Rechte und Pflichten
Artikel 53	§ 11 Abs. 1 und 2 Ernennung und Amtszeit
Artikel 54	§ 8 Errichtung
	§ 11 Ernennung und Amtszeit
	§ 12 Amtsverhältnis
	§ 13 Rechte und Pflichten
Abschnitt 2 Zuständigkeit, Aufgaben und Befugnisse	
Artikel 55	§ 9 Zuständigkeit
Artikel 56	§ 19 Zuständigkeiten
Artikel 57	§ 14 Aufgaben
Artikel 58	§ 16 Befugnisse
	§ 21 Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission
Artikel 59	§ 15 Tätigkeitsbericht
Kapitel VII Zusammenarbeit und Kohärenz	
Abschnitt 1 Zusammenarbeit	
Artikel 60	
Artikel 61	
Artikel 62	
Abschnitt 2 Kohärenz	
Artikel 63	
Artikel 64	
Artikel 65	
Artikel 66	
Artikel 67	
Abschnitt 3 Europäischer Datenschutzausschuss	
Artikel 68	§ 17 Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle
Artikel 69	
Artikel 70	

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
Artikel 71	
Artikel 72	
Artikel 73	
Artikel 74	
Artikel 75	
Artikel 76	
Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen	
Artikel 77	
Artikel 78	§ 20 Gerichtlicher Rechtsschutz
Artikel 79	§ 44 Klagen gegen den Verantwortlichen oder Auftragsverarbeiter
Artikel 80	
Artikel 81	
Artikel 82	
Artikel 83	§ 41 Anwendung der Vorschriften über das Bußgeld- und Strafverfahren
	§ 43 Bußgeldvorschriften
Artikel 84	§ 42 Strafvorschriften
Kapitel IX Vorschriften für besondere Verarbeitungssituationen	
Artikel 85	
Artikel 86	
Artikel 87	
Artikel 88	§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
Artikel 89	§ 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
	§ 28 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken
Artikel 90	
Artikel 91	
Kapitel X Delegierte Rechtsakte und Durchführungsrechtsakte	
Artikel 92	
Artikel 93	

Bestimmungen der VO (EU) 2016/679	Bestimmungen des BDSG
Kapitel XI Schlussbestimmungen	
Artikel 94	
Artikel 95	
Artikel 96	
Artikel 97	
Artikel 98	
Artikel 99	