SCHLÄGER • THODE (Hrsg.)

Handbuch Datenschutz und IT-Sicherheit

ESV ERICH SCHMIDT VERLAG

datenschutz nord GRUPPE

ERICH
SCHMIDT
VERLAG

Handbuch Datenschutz und IT-Sicherheit

Herausgegeben von

Dr. Uwe Schläger

Jan-Christoph Thode

Unter Mitarbeit von

Dr. Christian Borchers; Conrad S. Conrad; Michael Cyl; Dr. Sebastian Ertel; Annika Freund; Clemens Grünwald; Jennifer Jähn-Nguyen; Dr. Irene Karper; Jan-Roman Kitzinger; Dr. Martin Klein-Hennig; Dr. Bettina Kraft; Dr. Sanela Kühn; Dr. Sönke Maseberg; Dr. Britta Mester; Lars Meyer; Dr. M. J. Kolodziej; Christin Münzberg; Lea Paschke; Jan Peplow; Olaf Rossow; Jan Schirrmacher; Dr. Uwe Schläger; Felix Schmidt; Dr. Torge Schmidt; Markus Schönmann; Stefan R. Seiter; Daniel Stolper; Oliver Stutz; Jan-Christoph Thode; Sven Venzke-Caprarese; Ralf von Rahden

2., neu bearbeitete und erweiterte Auflage

ERICH SCHMIDT VERLAG

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

Weitere Informationen zu diesem Titel finden Sie im Internet unter
http://ESV.info/978-3-503-20533-2

Zitiervorschlag:
Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, 2. Aufl.

1. Auflage 2018
2. Auflage 2022

ISBN 978-3-503-20533-2 (gedrucktes Werk)
ISBN 978-3-503-20534-9 (eBook)

Druck: Hubert & Co., Göttingen

Vorwort

Rechtzeitig zum Inkrafttreten der EU-Datenschutz-Grundverordnung hatten wir im März 2018 erstmals unser Handbuch zum Datenschutz und zur IT-Sicherheit herausgegeben. Zielsetzung war es damals, Unternehmen, aber auch öffentlichen Stellen einen Werkzeugkasten an die Hand zu geben, um die Vorschriften der Datenschutz-Grundverordnung praxisgerecht umzusetzen und die Herausforderungen der Datenschutz-Grundverordnung zu bewältigen. Diese Zielsetzung ist auch mehr als drei Jahre nach Inkrafttreten der Datenschutz-Grundverordnung wichtiger denn je.

Nicht zuletzt aufgrund der deutlich erhöhten Bußgelder, die von Datenschutz-Aufsichtsbehörden bereits mehrfach verhängt wurden, sehen sich Unternehmen weiterhin mit enormen Herausforderungen konfrontiert: Neben erweiterten Informations-, Rechenschafts- und Meldepflichten gilt es, für Verfahren mit hohen Risiken für die Persönlichkeitsrechte der Betroffenen eine Datenschutz-Folgenabschätzung durchzuführen. Auftragsverarbeiter müssen ebenso wie Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen. Auch die Eignung technischer und organisatorischer Sicherheitsmaßnahmen muss regelmäßig überprüft und dokumentiert werden.

Die nunmehr vorliegende zweite Auflage unseres Handbuchs stellt eine inhaltlich überarbeitete Auflage dar, die sowohl auf zwischenzeitliche Urteile zum Datenschutz als auch auf Best-Practice-Ansätze Bezug nimmt, die sich in den letzten Jahren entwickelt und bewährt haben. Erstellt und aktualisiert wurde das Handbuch von erfahrenen Beraterinnen und Beratern der datenschutz nord Gruppe, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit als Consultant tätig sind.

Das vorliegende Datenschutz-Handbuch richtet sich an betriebliche Datenschutzbeauftragte, IT-Administratoren, Unternehmensleitungen, Betriebs- oder Personalräte, aber auch an datenschutzinteressierte Beschäftigte und Kunden, die sich entweder einen Überblick über die neuen gesetzlichen Regelungen verschaffen wollen oder praxisgerechte Vorschläge zur Umsetzung der Datenschutz-Grundverordnung nachlesen möchten.

Das Handbuch gliedert sich im Wesentlichen in zwei Hauptteile: Die Kapitel A bis F sind datenschutzrechtlich geprägte Kapitel, während die Kapitel G bis J sicherheitstechnische Aspekte in den Vordergrund stellen. Nachdem wir in Kapitel A zunächst auf die datenschutzrechtlichen Grundlagen eingehen, stellen wir in Kapitel B vor, wie ein betriebliches Datenschutz-Management umgesetzt werden sollte. In Kapitel C steht die gesetzeskonforme Verarbeitung von Beschäftigtendaten im Vordergrund, in Kapitel D die gesetzeskonforme Verarbeitung von Kundendaten. Kapitel E beschäftigt sich mit der Verarbeitung personenbezogener Daten im Internet, in sozialen Netzwerken und in unterneh-

menseigenen Intranets. Kapitel F stellt dar, in welchem Umfang Videosysteme nach der Datenschutz-Grundverordnung betrieben werden können.

Der zweite Hauptteil des Handbuches beginnt in Kapitel G mit einer Darstellung der rechtlichen Grundlagen der IT-Sicherheit. In Kapitel H werden die Eckpfeiler eines Informationssicherheits-Managements beschrieben. Kapitel I stellt geeignete technisch-organisatorische Maßnahmen vor, und zwar übergreifende Maßnahmen, Infrastrukturmaßnahmen, Maßnahmen seitens der IT-Systeme, Netzwerkmaßnahmen und Maßnahmen auf Anwendungsebene. Und schließlich wird in Kapitel J beschrieben, in welcher Form Penetrationstest zur Evaluierung einer angemessenen IT-Sicherheit durchgeführt werden können.

Trotz der zahlreichen Verweise auf andere Kapitel dieses Buches sind sämtliche Hauptkapitel in sich abgeschlossen und können separat ohne Kenntnis der anderen Kapitel als Erkenntnisquelle dienen.

In diesem Sinne wünschen wir Ihnen als Herausgeber dieses Datenschutz-Handbuchs viel Spaß beim Lesen und Nachschlagen.

Bremen und Berlin, im Oktober 2021 Uwe Schläger und Jan-Christoph Thode

Inhaltsverzeichnis

Bearbeiterverzeichnis

Dr. **Christian Borchers**	Teil C 9
Conrad S. Conrad	Teil E 1
Michael Cyl	Teil I 4, Teil J
Dr. **Sebastian Ertel**	Teil D 2
Annika Freund	Teil A 4.3
Clemens A. Grünwald	Teil E 3
Jennifer Jähn-Nguyen	Teil C 10
Dr. **Irene Karper**	Teil F
Jan-Roman Kitzinger	Teil A 1.3
Dr. **Martin Klein-Hennig**	Teil I 3
Dr. **Bettina Kraft**	Teil D 3
Dr. **Sanela Kühn**	Teil C 2
Dr. **Sönke Maseberg**	Teil I 1–1.3, Teil H
Dr. **Britta Mester**	Teil B 9
Lars Meyer	Teil I 1.4–1.6
Dr. **Martin Müller-Kolodziej**	Teil A 4–4.2
Christin Münzberg	Teil B 2, 4, 5, 7
Lea Paschke	Teil C 6
Jan Peplow	Teil A 3
Ralf von Rahden	Teil I 1.7
Olaf Rossow	Teil C 11

Jan Schirrmacher	Teil I 2
Dr. **Uwe Schläger**	Teil G, Teil I 1.8–1.9, 5
Felix Schmidt	Teil C 7–8, Teil D 4
Dr.-Ing. **Torge Schmidt**	Teil I 1.4–1.6
Markus Schönmann	Teil D 5
Stefan R. Seiter	Teil B 3, 6, Teil D 1
Daniel Stolper	Teil A 1–1.2, Teil C 3–5
Oliver Stutz	Teil B 1–8
Jan-Christoph Thode	Teil A 2, Teil C 1
Sven Venzke-Caprarese	Teil E 2

Abkürzungsverzeichnis

a. A.	andere Ansicht
a. E.	am Ende
a. F.	alte Fassung
Abs.	Absatz
Abschn.	Abschnitt
AEntG	Arbeitnehmer-Entsendegesetz
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
AO	Abgabenordnung
ArbZG	Arbeitszeitgesetz
Art.	Artikel
Aufl.	Auflage
Az.	Aktenzeichen
Bd.	Band
BDSG-alt	Bundesdatenschutzgesetz-alt
BDSG-neu	Bundesdatenschutzgesetz-neu
BEM	Betriebliches Eingliederungsmanagement
Beschl. v.	Beschluss vom
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CG	Corporate Governance
CMS	Compliance-Management-System
d. h.	das heißt
DAkkS	Deutsche Akkreditierungsstelle
DCGK	Deutsche Corporate Governance Kodex
DMZ	demilitarisierte Zonen
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSGVO	Datenschutzgrundverordnung
dt.	deutsch
EPVO/ePVO	ePrivacy-Verordnung
etc.	et cetera
EuGH	Europäische Gerichtshof
evtl.	eventuell

f./ff.	folgend/fortfolgend
Fn.	Fußnote
gem.	gemäß
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
grds.	Grundsätzlich
h. A.	herrschende Ansicht
HGB	Handelsgesetzbuch
h. M.	herrschende Meinung
Hrsg.	Herausgeber
Hs.	Halbsatz
i. d. F.	in der Fassung
i. d. R.	in der Regel
i. d. S.	in diesem Sinne
i. E.	im Ergebnis
inkl.	inklusive
i. R. d.	im Rahmen der/des
i. R. e.	im Rahmen einer/eines
i. R. v.	im Rahmen von
i. S. d.	im Sinne des/der
ISMS	Information Security Management System
i. S. v.	im Sinne von
i. Ü.	im Übrigen
i. V.	in Vertretung
i. V. m.	in Verbindung mit
KRITIS	Kritische Infrastrukturen
KSchG	Kündigungsschutzgesetz
KUG	Kunsturhebergesetz
KWG	Kreditwesengesetz
lit.	literra (= Buchstabe)
max.	maximal
m. E.	meines Erachtens
min.	minimal
Mio.	Millionen
Mrd.	Milliarden
m. w. N.	mit weiteren Nachweisen
MwSt.	Mehrwertsteuer
NachwG	Gesetz über den Nachweis der für ein Arbeitsverhältnis geltenden wesentlichen Bedingungen

n. F.	neue Fassung
Nr.	Nummer
o. a.	oben angegeben
o. ä.	oder ähnlich
o. Ä.	oder Ähnliches
o. g.	oben genannt
OWiG	Gesetz über Ordnungswidrigkeiten
p. a.	pro anno
Pos.	Position
pp.	per procura
RFID	radio-frequency identification
Rn.	Randnummer
Rs.	Rechtssache
Rspr.	Rechtsprechung
RStV	Rundfunkstaatsvertrag
s.	siehe
S.	Satz
s. a.	siehe auch
SchwarzArbG	Schwarzarbeitsbekämpfungsgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
ToMs	technische und organisatorische Maßnahmen
u. a.	unter anderem
u. Ä.	und Ähnliches
UAbs.	Unterabsatz
u. a. m.	und anderes mehr
u. E.	unseres Erachtens
Urt. v.	Urteil vom
usw.	und so weiter
u. U.	unter Umständen
UVV	Unfallverhütungsvorschriften
UWG	Gesetz gegen den unlauteren Wettbewerb
v. a.	vor allem
VAG	Versicherungsaufsichtsgesetz
vgl.	vergleiche
v. H.	von Hundert
Vorb.	Vorbemerkung
vs.	Versus

z. B.	zum Beispiel
Ziff.	Ziffer
zit.	zitiert
z. T.	zum Teil
zzgl.	zuzüglich

Literaturverzeichnis

Albrecht, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, S. 88.

Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2016.

Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019.

Bach, Datenschutzrechtliche Vorgaben bei der Weitergabe von Beschäftigten- und Kundendaten während der Due-Diligence-Phase, EuZW 2020, S. 175.

Becker, Personalentwicklung, Bildung, Förderung und Organisationsentwicklung in Theorie und Praxis, 6. Auflage 2013.

Born, Bonitätsprüfungen im Online-Handel (Scorewert-basierte automatisierte Entscheidung über das Angebot von Zahlungsmöglichkeiten), ZD 2015, S. 66.

Brehm, Verräterische Merkmale, c't 11/2016, S. 144.

Bussche v.d./Voigt, Konzerndatenschutz, 2. Auflage 2019.

Conrad/Hole, Datenschutzanforderungen bei einem Webseiten-Kontaktformular, K&R 2019, S. 761.

Däubler, Gläserne Belegschaften?, 5. Auflage 2010.

Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Auflage 2016.

Dehmel/Hullen, Auf dem Weg zu einem zukünftigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher, ZD 2013, S. 147.

Diepold/Loof, Implementierung von Hinweisgebersystemen, CB 2017, S. 25.

Edenfeld, Betriebsverfassungsrecht, 4. Auflage 2014.

Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017.

Engeler/Felber, Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, S. 251.

Erfurth, Der „neue" Arbeitnehmerdatenschutz im Bundesdatenschutzgesetz, NJOZ 2009, S. 2914.

Faust/Spittka/Wybitul, Milliardenbußgelder nach der DS-GVO? – Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, S. 120.

Fitting (Begr.)/Engels/Schmidt/Trebinger/Linsenmaier, Betriebsverfassungsgesetz, 28. Auflage 2016.

Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019.

Fuhlrott/Hoppe, Einstellungsuntersuchungen und Gentests von Bewerbern, ArbRAktuell 2010, S. 183.

Gola, Datenschutz-Grundverordnung, 2. Auflage 2018.

Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012.

Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015.

Gola/Wronka, Arbeitnehmerdatenverarbeitung beim Betriebs-/Personalrat und der Datenschutz, NZA 1991, S. 790.

Göpfert/Dußmann, Recruiting und Headhunting in der digitalen Arbeitswelt – Herausforderungen für die arbeitsrechtliche Praxis, NZA-Beilage 2016, S. 41.

Götz, Grenzüberschreitende Datenübermittlung im Konzern, DuD 2013, S. 631.

Greßlin, Umgang mit Bewerberdaten – was geht und was geht nicht?, BB 2015, S. 117.

Hahn/Vesting, Rundfunkrecht, 3. Auflage 2012.

Härting, Datenschutz-Grundverordnung, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016.

Hoeren/Siebert/Holznagel, Multimedia-Recht, 42. Ergänz. 2015.

Huff, Videoüberwachung im öffentlichen und privaten Bereich – eine Zwischenbilanz, JuS 2005, S. 896.

Jandt, Datenschutz durch Technik in der DS-GVO, DuD 2017, S. 562.

Jerchel/Schubert, Neustart im Datenschutz für Beschäftigte, DuD 2016, S. 782.

Jülicher/Röttgen/v. Schönfeld, Das Recht auf Datenübertragbarkeit – Ein datenschutzrechtliches Novum, ZD 2016, S. 358.

Kiesche, Datenschutz im BEM, RDV 2014, S. 321.

Klein/Roos, Videoüberwachung: Kostspielige Folgen für den Arbeitgeber? – Aktuelle Rechtsprechung – konkrete Bemessungsmaßstäbe, ZD 2016, S. 65.

Kort, Eignungsdiagnose von Bewerbern unter der Datenschutz-Grundverordnung (DS-GVO), NZA Beilage 2016, S. 62.

Krohm, Der Schutz personenbezogener Daten im Zuge von Unternehmenstransaktionen, 2012.

Kühling/Buchner, Datenschutz-Grundverordnung, 3. Auflage 2020.

Köhler/Bornkamm, UWG, 29. Auflage 2011.

Kühn/Schläger, Datenschutz in vernetzten Computersystemen, 1997.

Lachenmann, Datenübermittlung im Konzern, 2016.

Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage 2018.

Lepperhoff/Papendorf, Messenger im Unternehmen, RDV 2015, S. 309.

Makowicz/Bartosz, Die Deutschen und deren Compliance, CB 2015, S. 45.

Martin/Friedewald/Schiering/Mester/Hallinan/Jensen, Handbuch zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, 2020.

Martin/Mester/Schiering/Friedewald/Hallinan, Datenschutz-Folgenabschätzung: Ein notwendiges „Übel" des Datenschutzes?, DuD 2019, S. 149.

Momsen/Grützner, Wirtschafts- und Steuerstrafrecht, 2. Auflage 2020.

Moos, Datenschutz- und Datennutzungsverträge, 2. Auflage 2018.

Moos/Rothkegel, Nutzung von Scoring-Diensten im Online-Versandhandel (Scoring-Verfahren im Spannungsfeld von Bundesdatenschutzgesetz, AGG und DS-GVO), ZD 2016, S. 561.

Moosmayer, Compliance, 3. Auflage 2015.

Müller-Glöge/Preis/Schmidt, Erfurter Kommentar zum Arbeitsrecht, 21. Auflage 2021.

Ott, Die Impressumspflicht nach §§ 5 TMG, 55 RStV, MMR 2007, S. 354.

Öztürk, Arbeitnehmerüberlassung DS-GVO-konform lösen, DuD 2019, S. 143.

Paal/Pauly, Datenschutz-Grundverordnung, 3. Auflage 2021.

Pfeiffer, Schutz von Kundendaten im Rahmen von Unternehmenstransaktionen, DSRITB 2015, S. 245.

Plath, Datenschutzgrundverordnung/Bundesdatenschutzgesetz, 3. Auflage 2018.

Rauer/Ettig, Aktuelle Entwicklungen zum rechtskonformen Einsatz von Cookies – Die Rechtslage auf dem Prüfstand von Kommission und Gerichten, ZD 2016, S. 423.

Reinhard, Rechte und Pflichten des Betriebsrats bei der Verwendung von Arbeitnehmerdaten, Diss.: Hamburg 2012.

Reiserer/Christ/Heinz, Beschäftigten-Datenschutz und EU-Datenschutz-Grundverordnung, DStR 2018, S. 1501.

Roßmann, Grundlagen der EDV-Mitbestimmung, DuD 2002, S. 286.

Roßnagel, Europäische Datenschutz-Grundverordnung, 2016.

Sakuraba, Protection of Personal Information and Privacy in the Japanese Workplace, in: Japan Institute for Labour Policy and Training, Protection of Employees' Personal Information and Privacy, 2014.

Sander/Schumacher/Kühne, Weitergabe von Arbeitnehmerdaten in Unternehmenstransaktionen, ZD 2017, S. 105.

Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841.

Schantz/Wolff, Das neue Datenschutzrecht, 2017.

Schaub (Begr.)/Koch/Linck/Trebern/Vogelgesang, Arbeitsrechts-Handbuch, 18. Auflage 2019.

Schneider/Härting, Wird der Datenschutz nun endlich internettauglich? Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht, ZD 2012, S. 199.

Schröder, Datenschutzrecht für die Praxis, 3. Auflage 2019.

Schüßler/Zöll, EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz, DuD 2013, S. 639.

Seiter, Auftragsverarbeitung nach der Datenschutz-Grundverordnung, DuD 2019, S. 127.

Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014.

Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019.

Solove/Schwartz, Information Privacy Law, 5. Auflage 2014.

Sörup/Marquard, Auswirkungen der EU-Datenschutzgrundverordnung auf die Datenverarbeitung im Beschäftigungskontext, ArbR Aktuell 2016, S. 103.

Spelge, Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung, DuD 2016, S. 775.

Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage 2019.

Sydow, Datenschutzgrundverordnung, 2. Auflage 2018.

Taeger/Gabel, Datenschutzgrundverordnung/Bundesdatenschutzgesetz, 3. Auflage 2019.

Taeger/Rose, Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes, BB 2016, S. 819.

Taeger/Schweda, Die gemeinsam mit anderen Erklärungen erteilte Einwilligung, ZD 2020, 124.

Thode, Kundendaten beim Unternehmenskauf – tatsächlich ein Datenschutzproblem?, PinG 2016, S. 26.

Tinnefeld/Conrad, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, S. 391.

Veil, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, S. 3337.

Venzke-Caprarese, Durchblick im Cookie-Wirrwarr, c't 7/2016, S. 138.

Venzke-Caprarese, Retargeting in der Onlinewerbung, DuD 2017, S. 577.

Venzke-Caprarese, Social Media Monitoring Analyse und Profiling ohne klare Grenzen?, DuD 2013, S. 775.

Venzke-Caprarese, Standortlokalisierung und personalisierte Nutzeransprache mittels Bluetooth Low Energy Beacons, DuD 2014, S. 839.

Vogt, Compliance und Investigations – Zehn Fragen aus Sicht der arbeitsrechtlichen Praxis, NJOZ 2009, S. 4206–4220.

Warren/Brandeis, Harv. L. Rev. 4 (1890), S. 193.

Wehmeyer, Datenschutz und Übertragung von Kundendaten im Rahmen von Unternehmenstransaktionen, PinG 2014, S. 36.

Wennemann, TOM und die Datenschutz-Grundverordnung, DuD 2018, S. 174.

Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Auflage 2019.

Wirth/Krause, Whistleblowing – Universelles Instrument der Compliance?, CB 2015, S. 27.

Woitke, Das „Wie" der Anbieterkennzeichnung gemäß § 6 TDG, NJW 2003, S. 871.

Wronka/Gola/Pötters, Handbuch Arbeitnehmerdatenschutz, 7. Auflage 2016.

Wybitul, EU-Datenschutz-Grundverordnung in der Praxis – Was ändert sich durch das neue Datenschutzrecht?, BB 2016, S. 1077.

Wybitul, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? – Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen, ZD 2016, S. 203.

Wybitul, Das neue EU-Datenschutzrecht – Folgen für Compliance und interne Ermittlungen, CB 2016, S. 101.

Wybitul, Die EU-Datenschutz-Grundverordnung – hohe Bußgeldrisiken für Unternehmen, CB 2015, S. 1.

Kapitel A
Datenschutzrechtliche Grundlagen

1 Geschichte des Datenschutzrechts

Die Entwicklung des Datenschutzrechts setzt bereits ein, lange bevor sich die elektronische Datenverarbeitung in unserem Alltag durchgesetzt hat. Damit gehört der Datenschutz zu den wenigen Bereichen unserer technisierten Gesellschaft, die von Politik und Gesetzgebung bereits angegangen wurden, als der Öffentlichkeit und den Betroffenen ein entsprechender Regelungsbedarf und selbst der den Regelungsbereich kennzeichnende Begriff „Datenschutz" noch weitgehend unbekannt waren.[1] 1

1.1 Erste Entwicklungen

Die Anfänge systematischer Datensammlung gehen zunächst hauptsächlich auf den staatlichen Bereich zurück. Der Staat hatte seit jeher ein besonderes Interesse daran, möglichst viele Informationen über seine Bürger zu sammeln, sei es um diese leichter besteuern zu können oder um die Möglichkeit zu gewinnen, diese für den Militärdienst heranziehen zu können. Von Volkszählungen durch die Obrigkeit wird schon in der biblischen Weihnachtsgeschichte berichtet. Datenerhebungen durch private Stellen nahmen dann jedoch mit Ende des 19. Jahrhunderts stark zu, wobei hier vor allem geschäftliche Interessen im Vordergrund standen. 2

Erste „moderne" Diskussionen zum Thema Datenschutz kamen Anfang der 1960er Jahre in den USA auf und wurden unter dem Schlagwort „Privacy" geführt. Ausgangspunkt der Diskussion war auch hier wieder ein staatliches Handeln: In der US-Regierung unter John F. Kennedy gab es damals Planungen, ein „Nationales Datenzentrum" zur Verbesserung des staatlichen Informationswesens einzurichten. Vor dem Hintergrund, dass es in den USA weder flächendeckende Melderegister oder Meldewesen noch bundesweit geltenden Ausweise gibt, sollten dort die Daten aller US-Bürger registriert werden. Die Regierungspläne wurden in den nachfolgenden Debatten als Eingriff in das „right to be let alone" betrachtet, das bereits 1890 von Samuel D. Warren und dem späteren Bundesrichter Louis D. Brandeis entwickelt wurde. Die Autoren hatten in dem im „Harvard Law Review" veröffentlichten Artikel „The Right to Privacy" herausgearbeitet, dass jedem Individuum das Recht zustehe, selbst zu bestimmen, inwieweit seine „Gedanken, Meinungen und Gefühle" – mithin personenbezogene Informationen – anderen mitgeteilt werden sollten. Das Vorhaben der US-Regierung scheiterte letztlich im Kongress, woraufhin Forderungen nach gesetzlichen Grundlagen für die Verarbeitung personenbezogener Daten laut wurden. Es dauerte jedoch noch bis zum Jahr 1974, ehe der „Privacy Act" erlassen wurde. Das Gesetz enthielt Regelungen für die US-Bundesbehörden, die 3

1 Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015, Einl., § 4 Rn. 1.

sich bereits an wesentlichen Prinzipien des Datenschutzes orientierten, nämlich Erforderlichkeit, Sicherheit und Transparenz.[2]

4 Die amerikanische Debatte wurde auch in Europa verfolgt. Deutsche Rechtswissenschaftler begannen Ende der 1960er Jahre eine intensive Diskussion. In diesem Zusammenhang wurde auch der Begriff „Datenschutz" geschaffen, da eine unmittelbare Übersetzung des Begriffs „Privacy" wie „(allgemeines) Persönlichkeitsrecht" für den täglichen Gebrauch zu sperrig schien. Wegen des möglichen Missverständnisses (geschützt werden nicht die Daten, sondern die Menschen) wurde der Begriff „Datenschutz" anfänglich kritisiert. Inzwischen ist der Begriff aber selbst international gebräuchlich (vgl. engl. = „data protection", frz. = „protection des données", span. = „protección de datos" usw.).

5 Zu dieser Zeit wurde außerdem erstmals der Begriff des informationellen Selbstbestimmungsrechts geprägt. Dieser geht zurück auf ein Gutachten von Wilhelm Steinmüller, Bernd Lutterbeck und weiteren Bearbeitern aus dem Jahre 1971.[3] In diesem Gutachten wurde – ausgehend von der Annahme, dass mit Art. 2 Abs. 1 GG die allgemeine Handlungsfreiheit gewährleistet wird – hergeleitet, dass diese allgemeine Handlungsfreiheit „das Verfügungs- und damit das Zurückbehaltungsrecht bezüglich aller Individualinformationen umfasst, also als ‚informationelles Selbstbestimmungsrecht' zu verstehen ist".[4]

6 Diese Argumentation wurde später vom Bundesverfassungsgericht im so genannten Volkszählungsurteil[5] von 1983 übernommen. Das Volkszählungsurteil wird als eigentliche „Geburtsstunde des Datenschutzes" bezeichnet.[6] Das Urteil und seine Auswirkungen prägen das Datenschutzrecht in Deutschland bis heute.

1.2 Das Volkszählungsurteil des Bundesverfassungsgerichts

7 Der Gegenstand des Volkszählungsurteils war das sogenannte „Volkszählungsgesetz" (BGBl. I 1982, 369), mit dem der deutsche Gesetzgeber eine umfassende Volks-, Berufs-, Wohnung- und Arbeitsstättenzählung regeln wollte. Gegen die geplante Volkszählung regte sich großer Widerstand. Bereits in den 1980er Jahren war die elektronische Datenverarbeitung derart fortgeschritten, dass auch eine vermehrte Ausbreitung im privaten Bereich prognostiziert wurde. Dementsprechend zahlreich waren die Verfassungsbeschwerden, die gegen das Urteil erhoben wurden und die letztlich erfolgreich waren.

2 Abel, in: Roßnagel, Handbuch Datenschutzrecht, 2.7, B., II, 1. S. 198, Rn. 9.
3 Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, Juli 1971, BT-Drs. VI/3826, 5 ff.
4 Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, Juli 1971, BT-Drs. VI/3826, 4.1.4.
5 BVerfG, Urteil v. 15. 12. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83.
6 Vgl. Schröder, Datenschutzrecht für die Praxis, 2. Auflage, 1. Kapitel I 1.

1.2.1 Recht auf informationelle Selbstbestimmung

Im Volkszählungsurteil wurde vom Bundesverfassungsgericht die „informationelle Selbstbestimmung" als ein verfassungsrechtlich geschütztes Recht anerkannt. In der Begründung führte das Bundesverfassungsgericht aus, dass die Möglichkeiten der modernen Datenverarbeitung weithin nur noch für Fachleute durchschaubar seien und dass dies bei den Bürgern die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung auslösen könne. 8

Das Gericht hatte erkannt, dass personenbezogene Daten bereits zur Zeit des Urteilsspruchs „technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar"[7] waren. Würden diese untereinander verknüpft, entstünden weitgehend vollständige Persönlichkeitsbilder, deren Richtigkeit und Verwendung der Betroffene nicht mehr hinreichend kontrollieren könne. Hierdurch werde ein psychischer Druck auf jeden Einzelnen aufgebaut, der bereits für sich geeignet sei, auf das Verhalten des Einzelnen einzuwirken. Die individuelle Selbstbestimmung setze aber voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, könne in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.[8] 9

Zusammenfassend führt das Bundesverfassungsgericht in der Urteilsbegründung wie folgt aus: 10

> *„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. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 GG in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."*

7 BVerfG, Urteil v. 15. 12. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, S. 44, C. II. 1. a.
8 BVerfG, Urteil v. 15. 12. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, S. 44, C. II. 1. a.

11 Das Volkszählungsurteil führte zu weitreichenden Veränderungen in der Gesetzgebung, unter anderen einer späteren Novellierung des Bundesdatenschutzgesetzes. Seit dem Volkszählungsurteil war der Datenschutz ein wichtiger Bestandteil der Gesetzgebung. Für das heutige Verständnis und die Interpretation datenschutzrechtlicher Vorschriften ist es daher noch immer hilfreich, sich die Entstehungsgeschichte und die Aussagen des Volkszählungsurteils vor Augen zu führen.

1.2.2 Schutzbereich

12 Das Bundesverfassungsgericht sieht als Ausgangspunkt für das Recht auf informationelle Selbstbestimmung – also dem „Grundrecht auf Datenschutz" – das sogenannte allgemeine Persönlichkeitsrecht (APR) gem. Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG an.[9]

Das Recht auf informationelle Selbstbestimmung ist weit gefasst. Es umfasst die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Dabei wird nicht unterschieden, wie viele Daten insgesamt oder ob mehr oder weniger sensible Daten des Einzelnen betroffen sind. Das Bundesverfassungsgericht stellte fest, dass unter den Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen könne und es insoweit keine belanglosen Daten gebe.[10] Das Recht auf informationelle Selbstbestimmung erfasst sämtliche Daten mit Personenbezug und betrifft alle Formen der Erhebung und Verwendung.

1.2.3 Schranken

13 Einschränkungen des Rechts auf „informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Hierzu führte das Bundesverfassungsgericht aus:

> *„Dieses Recht auf ‚informationelle Selbstbestimmung' ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden […]. Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen."*[11]

9 BVerfG, Urteil v. 15. 12. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, S. 44, C. II.
10 BVerfG, Urteil v. 15. 12. 1983 – BvR 209, 269, 362, 420, 440, 484/83, S. 44, C. II. 2.
11 BVerfG, Urteil v. 15. 12. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, S. 46, C. II. 1. b.

Im Allgemeininteresse kann eine Verarbeitung personenbezogener Daten insbesondere dann liegen, wenn dies notwendig ist, um grundrechtliche geschützte Informationsrechte Dritter durchzusetzen. Diese können sich z. B. aus der Meinungsfreiheit gem. Art. 5 GG (bspw. personenbezogene Daten sind Gegenstand einer Meinungsäußerung), aus der Eigentumsgarantie gem. Art. 14 GG (personenbezogene Daten als Wirtschaftsgut) oder aus der allgemeinen Handlungsfreiheit gem. Art. 2 Abs. 1 GG ergeben. Grundrechte Dritter können jedoch nur in spezifischen Verarbeitungssituationen Einschränkungen im Schutzbereich des Rechts auf informationelle Selbstbestimmung rechtfertigen.

Einschränkungen bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Er darf die Datenverarbeitung nur gestatten, wenn sie zur Erreichung des angestrebten Zwecks geeignet, erforderlich und angemessen ist. Er hat daher den Eingriff in die informationelle Selbstbestimmung möglichst schonend zu gestalten.[12] Außerdem sind organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. 14

1.2.4 Weiterentwicklung des Rechts auf informationelle Selbstbestimmung

Auch nach dem Volkszählungsurteil war das informationelle Selbstbestimmungsrecht Gegenstand diverser Verfahren[13] vor dem Bundesverfassungsgericht, in denen es laufend weiterentwickelt und präzisiert wurde. 15

Im Jahr 2008 wurde dem informationellen Selbstbestimmungsrecht schließlich – als letzter großer Meilenstein – das „Recht auf Integrität informationstechnischer Systeme“ (welches tlw. als „Computergrundrecht“ bezeichnet wird) zur Seite gestellt, welches das Bundesverfassungsgericht ebenfalls aus dem allgemeinen Persönlichkeitsrecht ableitet. Der Schutzbereich des Grundrechts ist eröffnet, wenn ein Betroffener ein System als eigenes nutzt und nach den Umständen davon ausgehen darf, dass er allein oder mit anderen gemeinsam selbstbestimmt über das System verfügt und dem System personenbezogene Daten in einem Umfang anvertraut, die einen Einblick in wesentliche Teile der Lebensgestaltung seiner Person ermöglichen oder ein aussagekräftiges Bild über die Persönlichkeit zulassen,[14] bspw. zu den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers. Werden diese Daten von Dritten erhoben und ausgewertet, so könne dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.[15] 16

12 Simitis, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 1 Rn. 106.
13 Z. B. Beschluss vom 14. 12. 2000 – 2 BvR 1741/99 – „Genetischer Fingerabdruck“; Urteil vom 12. 04. 2005 – 2 BvR 581/01 – „GPS-Überwachung“; Beschluss vom 04. 04. 2006 – 1 BvR 518/02 – „Rasterfahndung“.
14 BVerfG, Urteil des Ersten Senats vom 27. 02. 2008 – 1 BvR 370/07, Rn. 206.
15 BVerfG, Urteil des Ersten Senats vom 27. 02. 2008 – 1 BvR 370/07, Rn. 178.

17 Das Bundesverfassungsgericht hatte erkannt, dass das Recht auf informationelle Selbstbestimmung im Zeitalter des Internets, in dem die meisten Betroffenen über eigene Computersysteme verfügen („vernetzte informationstechnische Systeme")[16], nicht mehr alleine ausreichend ist, um das allgemeine Persönlichkeitsrecht der Nutzer zu schützen:

> *„Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus."*[17]

18 Wenn ein Eingriff Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten, sei dieser Eingriff am „Recht auf Integrität informationstechnischer Systeme" zu messen.[18] Ein Eingriff liege vor, sobald die Möglichkeit eines Zugriffs auf die potentiell aussagekräftigen Datenbestände besteht.

1.2.5 Langfristige Bedeutung

19 Das informationelle Selbstbestimmungsrecht bindet – wie alle Grundrechte – zunächst den Gesetzgeber und stellt ein Abwehrrecht gegen den Staat dar. Zuerst wird für den Gesetzgeber also eine Grenze in seinen Befugnissen zur Datenverarbeitung gezogen. Darüber hinaus stellt das Recht auf informationelle Selbstbestimmung für den Gesetzgeber aber eine verbindliche Handlungsvorgabe dar.[19] Für diesen ergibt sich das Gebot zur Abwehr von Gefahren für das informationelle Selbstbestimmungsrecht, die dadurch entstehen, dass sowohl öffentliche als auch private Stellen Daten verarbeiten. Er muss sicherstellen, dass Einschränkungen des Rechts auf informationelle Selbstbestimmung nur dann erfolgen, wenn dies zur Wahrung der Rechte anderer erforderlich ist und wenn sie der verfassungsmäßigen Ordnung entsprechen. Im Rahmen der Gesetzgebung ergeben sich hieraus insbesondere das Gebot der Normenklarheit und der Verhältnismäßigkeit.[20]

16 BVerfG, Urteil des Ersten Senats vom 27. 02. 2008 – 1 BvR 370/07, Rn. 177.
17 BVerfG, Urteil des Ersten Senats vom 27. 02. 2008 – 1 BvR 370/07, Rn. 200.
18 BVerfG, Urteil des Ersten Senats vom 27. 02. 2008 – 1 BvR 370/07, Rn. 203.
19 Schmidt, in: Taeger, Bundesdatenschutzgesetz, 2. Auflage 2013, Einf. Rn. 45.
20 Simitis, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 1 Rn. 48.

Aufgrund der sogenannten „mittelbaren Drittwirkung der Grundrechte“ entfaltet das Recht auf informationelle Selbstbestimmung überdies seine Schutzwirkung nicht nur im Verhältnis zwischen Bürger und Staat, sondern auch im Verhältnis zwischen Privaten untereinander. Die Grundrechte sind insoweit als objektive Wertentscheidungen anzusehen, deren Wertungen bei der Auslegung von Generalklauseln und unbestimmten Rechtsbegriffen heranzuziehen sind.[21] Auch bei der Datenverarbeitung durch nicht-öffentliche Stellen sind die Wertungen des Rechts auf informationelle Selbstbestimmung daher zu berücksichtigen. 20

Im Ergebnis stellt die informationelle Selbstbestimmung den Maßstab und die Grundlage für die rechtliche Bewertung jeglicher Datenverarbeitung dar. Die daraus folgenden Rechte der Betroffenen sind zu beachten, unabhängig von gesetzlichen Vorschriften, wenn sie sich aus dem Recht auf informationelle Selbstbestimmung ergeben.[22] 21

1.3 Entwicklung der Datenschutzgesetze in Deutschland

Die Entwicklung des Datenschutzes in Deutschland ist untrennbar verbunden mit der Entwicklung der automatisierten Datenverarbeitung ab Mitte des 20. Jahrhunderts. Das Arbeiten mit Karteikartensystemen und Lochkartenautomaten wurde fortlaufend zeitintensiver und unwirtschaftlich. Die stetig zunehmenden Aufgaben der öffentlichen Daseinsvorsorge und die Notwendigkeit der Kommunikation zwischen den Behörden machten es notwendig, in der öffentlichen Verwaltung EDV-Anlagen zum Einsatz zu bringen. Diese EDV-Anlagen wurden immer weiter ausgebaut und vernetzt, mit der Folge, dass Anfang der 70er Jahre bereits erste Rechenzentren in Betrieb genommen wurden. Etwaige daraus resultierende datenschutzrechtliche Sorgen waren in Bevölkerung und Medien aber noch nicht verbreitet. 22

1.3.1 Bedarf an Datenschutzgesetzen

Eine Diskussion über den Schutz von persönlichen Daten kam erstmals im Jahre 1968 auf. Es gelangten die Pläne der damaligen Bundesregierung an die Öffentlichkeit, wonach beabsichtigt war, ein behördenübergreifendes EDV-System einzuführen, welches die Daten der Bürger, die zuvor noch in getrennten Systemen verwaltet wurden, zentral abrufbar machen sollte. Hierzu gehörte vor allem die Einführung einer individualisierten Personenkennziffer (bestehend aus der Zusammensetzung von Geburtsdatum, Geschlecht, einer vierstelligen Serienzahl zur Unterscheidung der am gleichen Tag geborenen Personen gleichen Geschlechts und einer Prüfziffer).[23] Die aufkommende Debatte drehte sich nun also um den Schutz der Privatsphäre jedes Einzelnen. Der steigende Einzug von EDV-Anlagen in der öffentlichen Verwaltung und die Einrichtung großer 23

21 BVerfG, NJW 1958, 257.
22 Simitis, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 1 Rn. 48.
23 BT-Dr. VI/598 vom 01. 04. 1970.

Datenbanken führten aber zu der Angst, dass der jeweilige Inhaber einer Datenbank ein informationelles Übergewicht gegenüber dem einzelnen Betroffenen erlangen würde. In der Literatur wurde bereits zu diesem Zeitpunkt darauf hingewiesen, dass was technisch betrachtet die elektronische Datenverarbeitung ausmacht, für den Einzelnen sowohl Chancen als auch Gefahren bewirke.[24] So waren wohl die Gefährdung der Privatsphäre und die befürchtete Informationsmacht der öffentlichen Stellen der Auslöser für den Ruf nach einem Datenschutzgesetz in Deutschland.

24 Der Ruf wurde dabei mit jedem technischen Fortschritt lauter und konsequenter. Waren es zu Beginn noch einzelne EDV-Anlagen, mit denen eine beschränkte Anzahl von Angestellten lokal die Daten verarbeiten konnten, so wurde die Datenverarbeitung durch die breite und alltägliche Anwendung von PCs, Laptops und Notebooks dezentralisiert und durch das Internet und die Entwicklung im Telekommunikationsbereich auf eine neue Stufe gehoben. Die Vernetzung durch das World Wide Web ermöglichte nun die Verknüpfung lokaler Rechner hin zu einem Netzwerk voller Datenströme. Das Internet holte immer mehr den Alltag in das Netz und durchdrang nun umso mehr sämtliche Lebensbereiche mit datenverarbeitenden Prozessen. Eine Vielzahl von Diensten ermöglichte es, dass das einfache Einstellen von Informationen in Netzwerken zu einem rasanten Anwachsen weltweiter Datenflüsse und Datenbestände führte.

25 Entsprechend der technischen Entwicklung erlangte also auch die Notwendigkeit des Schutzes der informationellen Selbstbestimmung und damit das Datenschutzrecht als modernes Rechtsgebiet eine stetig wachsende Bedeutung. Deutlich wird dies vor allem an der Entwicklung vom einstigen Landesdatenschutzgesetz hin zu einem harmonisierten Regelwerk für den europäischen Rechtsraum.

1.3.2 Landesdatenschutzgesetze

26 Die Diskussion über die aufkommenden Datenbanken staatlicher Behörden stärkten das Bestreben sich gegen die Informationsmacht des Staates zu stellen und die Privatsphäre des Einzelnen zu schützen. Die Bevölkerung in Deutschland schien überzeugt, dass die computerbasierte Datenverarbeitung durch öffentliche Stellen eine Begrenzung durch den Datenschutz erfahren müsse. Dies war die Geburtsstunde des Hessischen Datenschutzgesetzes, welches am 30. September 1970 verabschiedet wurde. Bei diesem Gesetz handelte es sich um das weltweit erste Datenschutzgesetz überhaupt, welches in seiner Ausarbeitung erstmals von „Datenschutz" sprach,[25] nachdem vormals in Deutschland immer vom Informationsschutz die Rede war. Das Gesetz richtete sich an die öffentlichen Stellen des Landes Hessen und enthielt eine Reihe von Maßnah-

24 Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, 673 ff.

25 Simitis, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, Einl. Rn. 2 m. w. N.

men, die die elektronisch verarbeiteten Daten vor dem Zugriff unbefugter Dritter schützen sollten. Darüber hinaus verankerte es das Datengeheimnis, schuf Rechte für die Betroffenen und führte die Institution des Datenschutzbeauftragten als Kontrollorgan für die öffentlichen Stellen des Landes ein.

Gefolgt vom Landesdatenschutzgesetz Rheinland-Pfalz (17. Januar 1974), gaben sich auch die anderen Bundesländer der alten Bundesrepublik im Laufe der Jahre ein Landesdatenschutzgesetz. Der Anwendungsbereich war dabei in allen Fällen identisch: Voraussetzung war stets die Verarbeitung personenbezogener Daten durch staatliche Stellen. Etwaige Regelungen für den privaten Bereich waren hingegen nicht vorhanden. 27

1.3.3 Bundesdatenschutzgesetz

Zeitlich zwischen den Landesdatenschutzgesetzen wurde durch den Bund ebenfalls ein Datenschutzgesetz erlassen, welches am 1. Februar 1977[26] im Bundesgesetzblatt verkündet wurde und an diesem Tag auch in wesentlichen Teilen in Kraft trat. Das Gesetz konzentrierte sich dabei ebenfalls auf den Schutz der personenbezogenen Daten. Im Gegensatz zu den Landesgesetzen wurde die Privatsphäre der Bürger aber nicht mehr allein als durch die öffentlichen Stellen bedroht angesehen, sondern auch durch die Privatwirtschaft. Der Anwendungsbereich bezog sich daher nicht nur auf die öffentlichen Stellen des Bundes, sondern ebenfalls auf die Datenverarbeitung privater Stellen. 28

Eine wesentliche Novellierung erfuhr das Bundesdatenschutzgesetz (BDSG) in Folge des „Volkszählungsurteils" des Bundesverfassungsgerichts vom 15. Dezember 1983.[27] Das Bundesverfassungsgericht stellte klar, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn der Betroffene eingewilligt hat oder ein Gesetz die Datenverarbeitung gestattet. Die Gesetzgeber wurden vom Bundesverfassungsgericht folglich aufgefordert Maßnahmen zu treffen, die das vom Bundesverfassungsgericht betonte Grundrecht auf informationelle Selbstbestimmung ausreichend schützten. Dies hatte zur Folge, dass nicht nur die Landesgesetzgeber, sondern auch der Bund sein Datenschutzgesetz anpassen musste. Mit der Novellierung des Bundesdatenschutzgesetzes im Jahre 1990 setzte schließlich auch der Bund die Vorgaben des Bundesverfassungsgerichts um. Dazu wurde in § 1 Abs. 1 BDSG 1990[28] über die Zweckbestimmung eingeführt, dass der Einzelne vor den Gefahren für das Persönlichkeitsrecht durch die Verarbeitung und Nutzung personenbezogener Daten geschützt werden sollte.[29] 29

Eine weitere, nach 1977 und 1990 dann dritte, Novellierung erfuhr das Bundesdatenschutzgesetz im Jahre 2001. Die europäische Union setzte mit der Daten- 30

26 BGBl. I S. 201.
27 Vgl. hierzu Kapitel A 1.2.
28 Bundesdatenschutzgesetz vom 20. 12. 1990, BGBl. I S. 2955 (verkündet als Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes).
29 Schmidt, in: Taeger/Gabel, Bundesdatenschutzgesetz, 2. Auflage 2013, § 1 Rn. 3.

schutzrichtlinie vom 24. Oktober 1995[30] neue datenschutzrechtliche Maßstäbe, die die Mitgliedstaaten innerhalb von drei Jahren in nationales Recht umzusetzen hatten. Ziel der Richtlinie war es den Datenaustausch innerhalb der Europäischen Gemeinschaft zu vereinfachen und einen datenschutzrechtlichen Mindeststandard zu schaffen. Zur Umsetzung der europäischen Datenschutzrichtlinie trat das geänderte Bundesdatenschutzgesetz am 23. Mai 2001[31] in Kraft.

31 Die letzte große Novelle erfuhr das BDSG im Jahre 2009. Grund für die Anpassung und Neueinführung von Regelungen im BDSG waren auftretende Skandale in der Privatwirtschaft mit Bezug zu Kunden- und Arbeitnehmerdaten. Inhaltlich wurde daher die Stellung des Datenschutzbeauftragten gestärkt, der Beschäftigten-Datenschutz mit § 32 BDSG-alt nun ausdrücklich geregelt und Anforderungen an den Adresshandel sowie an die Durchführung von Werbemaßnahmen aufgenommen. Die Vielzahl der Neuerungen trat am 01. 09. 2009[32] in Kraft.

32 Mit Wirksamwerden der Datenschutzgrundverordnung (DSGVO) verlor jedoch auch das BDSG sein bekanntes Gesicht. Wesentliche Regelungen des BDSG-alt wurden bereits von der DSGVO erfasst. Vollkommen obsolet wurde das nationale Datenschutzgesetz damit jedoch nicht. Hintergrund waren die verschiedenen „Öffnungsklauseln" in der Verordnung, die es den einzelnen Mitgliedstaaten ermöglichten bestimmte Sachverhalte konkreter zu regeln oder auch Rechte und Pflichten aus der Verordnung auf nationaler Ebene einzuschränken. Der deutsche Gesetzgeber machte mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUGEU vom 30. Juni 2017[33] davon Gebrauch. Das DSAnpUGEU hat das deutsche Datenschutzrecht an die ab Mai 2018 geltende DSGVO angepasst. Kernstück des Gesetzes war das – zum damaligen Zeitpunkt auch als „BDSG-neu" bezeichnete – grundlegend überarbeitete Bundesdatenschutzgesetz.[34]

1.3.4 Gesetzgebungskompetenz

33 Das Grundgesetz enthielt zwar mit Art. 10 – dem Grundrecht auf Wahrung des Brief-, Post- und Fernmeldegeheimnisses – eine Vorschrift mit datenschutzrechtlichem Bezug, nahm jedoch in keiner Regelung Stellung zur Zuständigkeit für die gesetzliche Regelung der Verarbeitung personenbezogener Daten. Für die Frage nach der Gesetzgebungskompetenz musste aus diesem Grund auf die Zuständigkeitsregelungen der Art. 70 ff. GG zurückgegriffen werden.[35] Nach Art. 70 Abs. 1 GG stand die Gesetzgebungskompetenz grundsätzlich den Bundes-

30 RL (EG) 95/46 v. 13. 10. 1994, ABl. EG Nr. L 281 S. 31–50 v. 23. 11. 1995; siehe hierzu auch Kapitel A 1.3.6.
31 BGBl. I S. 904.
32 BGBl. I S. 2814.
33 BGBl. I S. 2097.
34 Vgl. hierzu Kapitel A 2.1.2.
35 BT-Drs. 7/1072, S. 16; Simitis, in: Simitis, BDSG, 8. Auflage 2014, § 1 Rn. 1.

ländern zu, soweit eine Kompetenz nicht nach Maßgabe der Art. 71 ff. GG dem Bund übertragen wurde. Um die richtige Kompetenzgrundlage ermitteln zu können, musste nach dem konkreten Regelungszusammenhang gefragt werden. Demnach konnte sich der Bund bei der Datenverarbeitung durch private Unternehmen auf die konkurrierende Gesetzgebungskompetenz aus Art. 74 Abs. 1 Nr. 1, 11 und 12 GG stützen, da eine einheitliche Regelung des Datenschutzrechts zur Wahrung der Rechts- und Wirtschaftseinheit erforderlich war.[36] Neben den Regelungen für private Unternehmen enthielt das Bundesdatenschutzgesetz aber auch Vorschriften, die sich an die öffentliche Verwaltung des Bundes richteten (§§ 12 ff. BDSG-alt).

Für diesen Bereich gab es im Grundgesetz keine unmittelbar passende Kompetenzgrundlage. Eine solche konnte sich daher nur aus der Annexkompetenz zu Art. 73 und 72 GG ergeben. Dies war im Falle des Datenschutzrechts auch zu bejahen, wenn öffentliche Stellen personenbezogene Daten im Zusammenhang mit einer Materie bearbeiteten, für die eine Bundeskompetenz bestand.[37] Auch für das Verwaltungsverfahren bzw. das gerichtliche Verfahren ließ sich für die Datenverarbeitung durch öffentliche Stellen eine Regelungskompetenz des Bundes aus Art. 74 Abs. 1 Nr. 1 GG entnehmen. Im Ergebnis blieb damit für jedes Bundesland nur die Regelung der normativen Anforderungen an die Verarbeitung personenbezogener Daten für „seine" öffentlichen Stellen übrig. Dies galt aber auch nur für diejenigen öffentlichen Stellen und – ggf. privatrechtlichen – Vereinigungen, deren Tätigkeit in der Wahrnehmung der Aufgaben der öffentlichen Verwaltung bestand.[38] Im Übrigen oblag die Gesetzgebungskompetenz dem Bund. 34

1.3.5 Verhältnis Bundesdatenschutzgesetz – Datenschutzgesetze der Länder

Der Anwendungsbereich des BDSG-alt ergab sich aus dessen § 1 Abs. 2. Demnach waren Normadressaten grundsätzlich die öffentlichen Stellen des Bundes, öffentliche Stellen der Länder sowie die nicht-öffentlichen Stellen. Das Gesetz erfasste damit den gesamten Bereich der öffentlich-rechtlichen Verwaltung des Bundes sowie Unternehmen der Privatwirtschaft. Ins Leere ging die Regelung jedoch in Bezug auf die öffentlichen Stellen der Länder. Zwar fielen diese über § 1 Abs. 2 Nr. 2 in den Anwendungsbereich des BDSG-alt, dies jedoch nur, sofern der Datenschutz nicht durch Landesrecht geregelt war. Es hatten jedoch alle 16 Bundesländer von der Möglichkeit Gebrauch gemacht, sich ein eigenes Landesdatenschutzgesetz zu geben. Die daraus resultierende Subsidiarität des BDSG-alt erfuhr durch den Ausdruck „soweit" in § 1 Abs. 2 BDSG-alt aber wiederum eine Einschränkung. Die Datenschutzgesetze der Länder gingen nur insoweit 35

36 Gola/Klug, Grundzüge des Datenschutzrechts, 2. Auflage 2013, S. 8.; Taeger/Schmidt, in: Taeger/Gabel, Bundesdatenschutzgesetz, Einf. Rn. 7.

37 Taeger/Schmidt, in: Taeger/Gabel, Bundesdatenschutzgesetz, 2. Auflage 2013, Einf. Rn. 8; Simitis, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 1 Rn. 13.

38 Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015, § 1 Rn. 19a.

vor, als dass sie eine eigene Regelung enthielten. Hierfür kam es aber nicht auf die Frage an, ob die Regelung des Landesdatenschutzgesetzes mit der des BDSG-alt übereinstimmte oder ob sie für den Betroffenen günstig oder weniger günstig war.[39] Wenn die Landesdatenschutzgesetze keine eigenständige Regelung enthielten, wurde das BDSG-alt durch sie auch nicht verdrängt, es sei denn, die Nichtregelung erfolgte bewusst und erkennbar.

1.3.6 Europarechtliche Regelungen

36 Zu keiner Zeit war die europäische Prägung des Datenschutzes so sichtbar, wie heute durch die DSGVO. Dabei ist der europäische Einfluss auf das – auch deutsche – Datenschutzrecht nicht neu. Die rechtliche Beurteilung des Datenschutzes wurde bereits seit Beginn der Datenschutzregulierung von zahlreichen europäischen Regelungen geprägt. Die nachfolgende Darstellung gibt einen Überblick über die bedeutendsten Rechte und Rechtsakte.

EU-Grundrechte

37 An erster Stelle innerhalb der Normenhierarchie der Europäischen Union steht die Grundrechtecharta als Teil des EU-Primärrechts. Über den Vertrag über die Europäische Union ist sie zu geltendem Primärrecht geworden, Art. 6 Abs. 1 EUV. Ihrem Anwendungsbereich nach (Art. 51 Abs. 1 EU-Grundrechtecharta) richtet sie sich sowohl an die Europäische Union selbst, wie auch an die einzelnen Mitgliedstaaten,[40] wenn diese Unionsrecht durchführen. Letzteres kann etwa die Umsetzung einer Richtlinie oder die unmittelbare Vollziehung eines Beschlusses sein.

38 In Art. 8 normiert die EU-Grundrechtecharta ein explizites Datenschutzgrundrecht. Demnach hat jede Person „das Recht auf den Schutz der sie betreffenden personenbezogenen Daten“ (Art. 8 Abs. 1 EU-Grundrechtecharta). Darüber hinaus dürfen die personenbezogenen Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken“ (Art. 8 Abs. 2 EU-Grundrechtecharta).

39 Der Aufbau der EU-Grundrechte ist dabei identisch zu dem der im Grundgesetz verankerten Rechte: auf erster Stufe ist der Schutzbereich des jeweiligen Grundrechts zu bestimmen. Danach ist zu prüfen, ob ein Eingriff in diesen Schutzbe-

39 Simitis, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 1 Rn. 125.

40 Die Grundrechtecharta gilt nicht uneingeschränkt in allen Mitgliedstaaten. Für Großbritannien und Polen wurde nach dem „Protokoll Nr. 30 zum Lissaboner Vertrag über die Anwendung der Charta der Grundrechte der Europäischen Union auf Polen und das Vereinigte Königreich“ eine Ausweitung der Befugnisse des EuGH und der nationalen Gerichte zur Feststellung der Grundrechtswidrigkeit nationaler Maßnahmen und die Begründung einklagbarer Rechte aufgrund der Grundrechtecharta ausgeschlossen.

reich stattgefunden hat und ob dieser gerechtfertigt werden kann. Der Schutzbereich von Art. 8 Abs. 1 EU-Grundrechtecharta umfasst alle Informationen über eine bestimmte oder bestimmbare Person. Es macht dabei keinen Unterschied, ob es sich um eine natürliche oder juristische Person handelt. Für die juristische Person kommt es lediglich darauf an, dass das Grundrecht auf diese wesensmäßig anwendbar ist, wenn also bspw. der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt und es sich nicht nur um reine Geschäftsdaten handelt.[41] Ein Eingriff in dieses Grundrecht liegt immer dann vor, wenn personenbezogene Daten verarbeitet werden und dieser Eingriff nicht durch eine gesetzlich geregelte legitime Grundlage gerechtfertigt ist.

Neben Art. 8 EU-Grundrechtecharta kennt das europäische Primärrecht eine weitere bedeutende Rechtsquelle für das Datenschutzrecht: Art. 16 AEUV. Es handelt sich hierbei um eine korrespondierende Vorschrift zu Art. 8 EU-Grundrechtecharta. Der Art. 16 AEUV sieht als Grundsatzbestimmung vor, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. In Absatz zwei ist weiterführend eine Rechtsgrundlage für den Erlass sekundärrechtlicher Regelungen vorhanden. Als Adressaten des Datenschutzes sind neben den Organen der Union vor allem auch die Mitgliedstaaten genannt, soweit es sich um Tätigkeiten handelt, die in den Anwendungsbereich des Unionsrechts fallen oder den freien Datenverkehr betreffen. 40

Im Fall des Datenschutzrechts ergibt sich also die besondere Situation, dass das Datenschutzgrundrecht – anders als die übrigen Grundrechte – außerhalb der EU-Grundrechtecharte ein zweites Mal hervorgehoben wird. Dies führt für die Anwendung unweigerlich zu der Frage, ob bei der Beschränkung des Grundrechts der schrankenlose Art. 16 Abs. 1 AEUV gilt oder Art. 8 Abs. 2 EU-Grundrechtecharta, was im Ergebnis aber zu Gunsten des Art. 8 EU-Grundrechtecharta zu entscheiden ist.[42] 41

Zuletzt enthält auch Art. 8 EMRK einen datenschutzrechtlichen Anknüpfungspunkt. So ist zwar das Grundrecht auf informationelle Selbstbestimmung Teil der Garantie des Art. 8 EMRK, die Vorschrift selbst jedoch aber nicht datenschutzspezifisch, weshalb es für die Anwendbarkeit einer Entsprechung von Art. 8 EU-Grundrechtecharta fehlt.[43] Die Vorschrift der EMRK und insbesondere die Rechtsprechung des EGMR hierzu sind jedoch dann von erheblicher Bedeutung, wenn es darum geht, das Datenschutzgrundrecht mit Leben zu füllen. 42

Im Ergebnis ist damit Art. 8 EU-Grundrechtecharta der maßgebliche Ausgangspunkt für das Grundrecht auf Datenschutz, welches in seiner Anwendung durch die vielseitigen Rechtsakte der Union beeinflusst wird. 43

41 Kühling/Seidel/Sivridis, Datenschutzrecht, 3. Auflage 2015, S. 17; Knecht, in: Schwarze, EU-Kommentar, 3. Auflage 2012, Art. 8 GRC, Rn. 3.

42 Bernsdorff, in: Meyer, Charta der Grundrechte der Europäischen Union, 4. Auflage 2014, Art. 8, Rn. 17; Kingreen, in: Callies/Ruffert, EUV/AEUV, 5. Auflage 2016, Art. 16 AEUV, Rn. 3, Art. 8 EU-Grundrechtecharta, Rn. 3.

43 Kingreen, in: Callies/Ruffert, EUV/AEUV, 5. Auflage 2016, Art. 8 EU-Grundrechtecharta, Rn. 4.

Primär- und Sekundärrecht

44 Bei den datenschutzrechtlichen Anknüpfungspunkten in der EU-Grundrechtecharta und dem AEUV handelt es sich bei der Normenhierarchie um das sogenannte Primärrecht. Dies sind in erster Linie die Gründungsverträge (EUV und AEUV einschließlich derer Anhänge und Protokolle), erfasst jedoch auch die ungeschriebenen Rechtsgrundsätze des Unionsrechts sowie die EU-Grundrechtecharta. Ähnlich dem innerstaatlichen Verhältnis von Grundgesetz zu einfachem Gesetz gebührt dem Primärrecht Vorrang vor den übrigen europarechtlichen Vorschriften, weshalb es oftmals auch als „Verfassung der Europäischen Union" bezeichnet wird.[44]

45 Das Sekundärrecht hingegen erfasst alle Rechtsakte, die Unionsorgane aufgrund der primärrechtlichen Verträge oder aufgrund einer Ermächtigung durch einen anderen Rechtsakt erlassen haben. Im Wesentlichen handelt es sich dabei um Verordnungen oder Richtlinien. Die Verordnung ist ein Rechtsakt des Rates und der Kommission, deren Merkmal darin besteht, dass sie allgemeine Geltung hat, in allen ihren Teilen verbindlich ist und unmittelbar in jedem Mitgliedstaat gilt (Art. 288 Abs. 2 AUEV). Richtlinien hingegen wenden sich nach Art. 288 Abs. 4 AEUV nur an die Mitgliedstaaten und bedürfen einer Umsetzung in das nationale Recht. Die wichtigsten Rechtsakte auf europäischer Ebene mit datenschutzrechtlichem Bezug werden im Folgenden dargestellt.

Datenschutz-Richtlinie 95/46/EG

46 Auf der Ebene des Sekundärrechts prägte die Datenschutz-Richtlinie 95/46/EG vom 24. 10. 1995 (EG-DSRL) das BDSG-alt in seiner letzten Ausgestaltung am intensivsten. Ziel der Richtlinie war die europaweite Harmonisierung des Datenschutzstandards.

47 Allgemein gilt in der Europäischen Union der Grundsatz, dass die Institutionen der EU, also die Europäische Kommission, der Rat oder auch das Europäische Parlament, sich selbst keine Zuständigkeiten zuschreiben können. Die EU kann nur diejenigen Rechtsetzungskompetenzen an sich ziehen, für die die Mitgliedstaaten ihre vertragliche Einwilligung erteilt haben (sogenanntes Prinzip der begrenzten Einzelermächtigung, Art. 5 Abs. 1 EUV). Für die Frage nach der Rechtsetzungskompetenz war daher die in den Verträgen geregelte Kompetenzverteilung von entscheidender Bedeutung. Zu unterscheiden sind dabei einerseits die ausschließliche Kompetenz der EU (Art. 2 Abs. 1 AEUV), wonach in abschließend aufgezählten Bereichen die Mitgliedstaaten nicht mehr handlungsbefugt sind Gesetze zu erlassen, unabhängig davon, ob die EU von der Rechtsetzungsbefugnis Gebrauch gemacht hat und andererseits die geteilten Zuständigkeiten (Art. 2 Abs. 2 AEUV). Nach letzterer – auch als konkurrierend bezeichneter – Zuständigkeit sind die Mitgliedstaaten nur insoweit und solange zuständig, wie die EU noch keine Rechtsakte erlassen hat, die die Materie abschließend regeln. Die Kompetenz für den Erlass der Datenschutzrichtlinie

44 Streinz, Europarecht, 10. Auflage 2016, Rn. 448.

wurde auf die Binnenmarktharmonisierungskompetenz aus Art. 114 AEUV gestützt.[45] Dabei handelt es sich um eine geteilte Zuständigkeit.[46]

Das Kernstück der Richtlinie ergibt sich aus Art. 1 Abs. 2 EG-DSRL. Dieser sieht vor, dass die Mitgliedstaaten den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten nicht aus Datenschutzgründen untersagen dürfen. Dies verdeutlicht wiederum die Absicht des Gesetzgebers, einen einheitlichen Datenschutzstandard zu schaffen. Im Weiteren ähnelt die Richtlinie von der Struktur her stark der des alten Bundesdatenschutzgesetzes. 48

So wurde beispielsweise der Mechanismus zur Zulässigkeit einer Datenverarbeitung dem BDSG-alt entnommen, indem Art. 7 EG-DSRL als Legitimationsgrundlage neben der Einwilligung gleichranging auf die Verwirklichung berechtigter Interessen abstellt. Des Weiteren stärkte auch die Richtlinie u. a. den Grundrechtschutz der Betroffenen, indem sie ihnen verschiedene Rechte zustand (Recht auf Zugang zu Daten, Recht auf Information über Daten, das Recht, Daten zu berichtigen sowie auch das Recht, unter gewissen Voraussetzungen Löschung oder Sperrung zu verlangen; Art. 12 EG-DSRL), enthielt Vorschriften zur Verarbeitung von sensiblen Daten (Art. 8 EG-DSRL) und sah in Art. 25 EG-DSRL eine Regelung zur Weitergabe von Daten an Verarbeiter in Drittländern vor, die kein ausreichendes Schutzniveau bieten. 49

Nach Art. 29 der EG-DSRL wurde zudem eine Arbeitsgruppe zur Förderung der grenzüberschreitenden Zusammenarbeit in Datenschutzsachen ins Leben gerufen. Die sogenannte Artikel 29-Gruppe war ein unabhängiges Beratungsgremium der Europäischen Union für alle Fragen rund um den Datenschutz.[47] Sie bestand aus je einem Vertreter der jeweiligen Aufsichtsbehörde der einzelnen Mitgliedstaaten. Zu deren Aufgabe gehörte unter anderem bei der Umsetzung der EG-DSRL in den Mitgliedstaaten beizutragen wie auch die Beratung der Kommission bei allen Fragen rund um das Thema Datenschutz. Ihr oblag es auch, eine einheitliche Anwendung der unionsrechtlichen Datenschutzvorgaben in den Mitgliedstaaten zu fördern und die Zusammenarbeit der nationalen Aufsichtsbehörden zu stärken. 50

Die EG-DSRL machte den Mitgliedstaaten die Vorgabe, ihre Inhalte innerhalb einer Frist von 3 Jahren umzusetzen. Obgleich diese Frist also am 24. Oktober 1998 abgelaufen war, schaffte es die Bundesrepublik Deutschland nicht, die EG-DSRL in nationales Recht umzusetzen. Dies erfolgte erst mit der Neuformulierung des Bundesdatenschutzgesetzes im Jahre 2001. Mit der damaligen Neuausrichtung hielten auch viele bekannte Grundsätze des „modernen Daten- 51

45 Kühling/Seidel/Sivridis, Datenschutzrecht, 3. Auflage 2015, S. 23; Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Auflage 2012, S. 85.

46 Korte, in: Callies/Ruffert, EUV/AEUV, 5. Auflage 2016, Art. 114 AEUV, Rn. 8.

47 Die Artikel 29-Gruppe wurde zum 25. Mai 2018 durch den Europäischen Datenschutzausschuss (EDSA) ersetzt. Der EDSA verfolgt in gleicher Weise das Ziel, die einheitliche Anwendung der DSGVO sicherzustellen und die Zusammenarbeit zwischen den Datenschutzbehörden der Europäischen Union zu fördern.

schutzrechts“[48] Einzug in das alte Bundesdatenschutzgesetz, wie bspw. der Grundsatz der Datenvermeidung und Datensparsamkeit und des Datenschutzes durch Technik. Mit aufgenommen wurden außerdem Vorschriften zur Übermittlung von personenbezogenen Daten ins Ausland und Regelungen zur Videoüberwachung.

Weitere europarechtliche Vorschriften

52 Im Februar 2001 trat die **Verordnung (EG) Nr. 45/2001** des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr in Kraft. Die Verordnung enthält Regelungen, die in wesentlichen Teilen mit den Vorschriften der EG-DSRL übereinstimmen. So finden sich Vorschriften zu den Voraussetzungen der Zulässigkeit einer Datenverarbeitung wieder, wie auch die Rechte der Betroffenen. Gleichfalls sorgte die Verordnung in der europäischen Datenschutzarchitektur für eine institutionelle Kontrollinstanz: jedes Organ und jede Einrichtung der Europäischen Gemeinschaft hatte einen Datenschutzbeauftragten zu bestellen. Darüber hinaus wurde als unabhängige Kontrollbehörde das Amt eines europäischen Datenschutzbeauftragten eingerichtet. Der europäische Datenschutzbeauftragte berät und überwacht unabhängig und weisungsfrei die europäischen Organe und Einrichtungen und ist Mitglied des Europäischen Datenschutzausschusses.

53 Die Richtlinie über die „Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ vom 12. Juli 2002 (**RL 2002/58/EG,** sogenannte E-Privacy-RL) enthält sektorspezifische Regelungen für den Bereich der elektronischen Kommunikation. Ziel der Richtlinie ist es insbesondere das Recht auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten. Im Gegensatz zur EG-DSRL soll nicht nur der Schutz natürlicher Personen gewährleistet werden, sondern die Richtlinie weitet den Anwendungsbereich auf den Schutz berechtigter Interessen juristischer Personen aus, Art. 1 Abs. 2 S. 2 RL 2002/58/EG. Kernstück der Richtlinie ist die in Art. 5 RL 2002/58/EG enthaltene Vertraulichkeit der Kommunikation. So ist nach Art. 5 Abs. 1 S. 2 insbesondere das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und Verkehrsdaten ohne Einwilligung des Betroffenen nicht erlaubt. Ferner beinhaltet Art. 5 Abs. 3 RL 2002/58/EG erstmalig eine Regelung zum Einsatz sogenannter „Cookies“. Der Einsatz solcher Instrumente, die dazu geeignet sind Daten vom Endgerät des Nutzers auszulesen, ist demnach immer dann erlaubt, wenn der Nutzer über den Einsatz dieser technischen Hilfsmittel vorab vollständig und verständlich informiert wird und auf das Recht hingewiesen wird, die Verarbeitung zu verweigern (sogenanntes „Opt-

48 Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015, Einleitung, Rn. 12.

out-Prinzip"). Die dritte wesentliche Regelung findet sich in Art. 9 Abs. 1 S. 1 RL 2002/58/EG wieder. Hierbei geht es um die Nutzung von Standortdaten, deren Speicherung und Verarbeitung nur nach Anonymisierung oder Einwilligung des Nutzers zulässig ist. Die Bundesregierung hatte diese Richtlinie im Jahre 2004 mit einer Novellierung des Telekommunikationsgesetzes umgesetzt.

Die in die Jahre gekommene E-Privacy-Richtlinie sollte ursprünglich ab 2018 durch eine neue E-Privacy-Verordnung abgelöst werden. Der Entwurf der Verordnung sah vor, dass der Anwendungsbereich immer dann eröffnet sein soll, wenn es um die Verarbeitung elektronischer Kommunikationsdaten im Zusammenhang mit der Bereitstellung und Benutzung elektronischer Kommunikationsdienste geht. Die Verordnung würde dann für den Bereich der digitalen Dienste speziellere Regelungen als die DSGVO enthalten, so dass die DSGVO immer dann zurücktreten würde, wenn die E-Privacy-Verordnung Anwendung fände. Inhaltlich sollten u. a. die Regeln für den Umgang mit Cookies vereinfacht, die Regelungen für Direktmarketing verschärft sowie die Datensicherheit für Kommunikationsdienste wie WhatsApp, Facebook Messanger oder Skype ausgeweitet werden. Der Zeitplan sah vor, dass die E-Privacy-Verordnung bereits im Mai 2018 in Kraft treten sollte. Hierzu legte die Kommission Anfang 2017 ihren bereits einmal überarbeiteten Entwurf der Verordnung[49] vor, der anschließend im Europäischen Parlament diskutiert und von einem Entwurf des Präsidenten des Rats der Europäischen Union begleitet wurde. Seitdem steckte der Entwurf allerdings in der dritten Instanz, dem Rat der Europäischen Union, fest. Die Mitgliedstaaten konnten sich inhaltlich nicht auf einen gemeinsamen Nenner einigen. Angesichts dieser Uneinigkeit der Mitgliedstaaten kündigte die Kommission 2019 die Ausarbeitung eines neuen Entwurfes der E-Privacy-Verordnung an, mit dem der gesamte Entscheidungsprozess aber nochmals von vorne beginnen wird. Das Inkrafttreten der E-Privacy-Verordnung wird aus diesem Grund noch einige Jahre dauern, würde dann aber in jedem Fall die Datenschutzreform durch die DSGVO abrunden. 54

Eine weitere Richtlinie, die im Zusammenhang mit dem Datenschutz steht, ist die Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, vom 15. März 2006 **(Vorratsdatenspeicherungsrichtlinie 2006/24/EG).** Sie hat das Ziel sicherzustellen, dass bestimmte Daten der elektronischen Kommunikation zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen. Welche Datenarten von den Telekommunikationsanbietern vorgehalten werden müssen, ergibt sich aus Art. 5 Abs. 1 RL 2006/24/EG. Allgemein geht es dabei um die Speicherung der Verkehrs- und Standortdaten sowohl juristischer als auch natürlicher Personen. Darüber hinaus fallen alle damit in Zusammenhang stehenden Daten unter den Anwendungsbereich der 55

49 COM (2017) 10 final.

Richtlinie, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind (z. B. IP-Adressen, Verbindungsdaten, Kennung von Funkzellen etc.). Von der Vorratsdatenspeicherung ausgeschlossen werden jedoch der Inhalt der elektronischen Nachrichtenübermittlung, einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden.

56 Der deutsche Gesetzgeber hatte diese Richtlinie im Jahre 2008 in die nationalen Gesetze umgesetzt. Das Bundesverfassungsgericht erklärte 2010 jedoch die Regelungen zur Vorratsdatenspeicherung als nicht mit dem Grundgesetz vereinbar.[50] Das Bundesverfassungsgericht sah in den Vorschriften einen Verstoß gegen das in Art. 10 GG niedergelegte Fernmeldegeheimnis. Das Gericht betonte aber gleichermaßen, dass eine Vorratsdatenspeicherung nicht per se unzulässig sei. Sie müsse sich lediglich vielmehr an einer Reihe enger Vorgaben zur Verwendung der Daten, zur Sicherheit bei der Speicherung sowie zur Transparenz bei der Verwendung halten. Danach wurde diese Richtlinie nicht erneut in das deutsche Recht umgesetzt und 2014 entfiel die Umsetzungspflicht durch ein Urteil des EuGH.

57 Die Richter des EuGH hatten zu prüfen, ob die RL 2006/24/EG mit der EU-Grundrechtecharta zu vereinbaren ist. Es erfolgte eine Prüfung der Richtlinie mit der Vereinbarkeit von Art. 7 EU-Grundrechtecharta – der Achtung des Privat- und Familienlebens – sowie mit Art. 8 EU-Grundrechtecharta – dem „Datenschutzgrundrecht". Dabei kam der Gerichtshof zu dem Ergebnis, dass die genannten Grundrechte durch die RL 2006/24/EG in einem nicht erforderlichen Maße eingeschränkt werden und der Unionsgesetzgeber die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit hätte einhalten müssen. Zwar sei die Bekämpfung der schweren Kriminalität ein dem Gemeinwohl dienendes Ziel, für das die Vorratsdatenspeicherung auch grundsätzlich geeignet sei, jedoch fehle es an klaren und präzisen Regeln zur Tragweite des Eingriffes in die genannten Grundrechte. Der EuGH hat damit die Richtlinie 2006/24/EG für ungültig erklärt.[51]

58 Die Bundesregierung hat in Folge des Urteils die Regelungen[52] zur Vorratsdatenspeicherung novelliert. Die Änderungen traten Mitte Dezember 2015[53] in Kraft und beinhalteten detaillierte Regelungen zur Speicherung von Rufnummer, IP-Adressen und Zeitpunkten der Kommunikation. In seinem Urteil[54] vom 21. 12. 2016 hat der EuGH jedoch erneut im Wege eines Vorabentscheidungsverfahrens entschieden, dass die Mitgliedstaaten den Betreibern elektronischer Kommunikationsdienste keine allgemeine Verpflichtung zur Vorratsdatenspeicherung auferlegen dürfen. Der EuGH stellte fest, dass aus der Gesamtheit von gespeicherten Kommunikationsdaten sehr genaue Rückschlüsse auf das Privat-

50 BVerfG v. 02. 03. 2010 – 1 BvR 256/08, BVerfGE 125, 260.
51 EuGH v. 08. 04. 2014 – verb. Rs. C-293/12 und C-594/12 – Slg. 2014, 44.
52 Die Pflichten zur Vorratsdatenspeicherung sind in den §§ 113a–113g TKG geregelt.
53 „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" vom 10. Dezember 2015, BGBl. I S. 2218.
54 EuGH v. 21. 12. 2016 – verb. Rs. C-203/15 und C-698/15.

leben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden können. Eine nationale Regelung, die eine Speicherung von Verkehrs- und Standortdaten vorsieht, stellt aus diesem Grund einen besonders schwerwiegenden Grundrechtseingriff dar. Rechtfertigung für einen Eingriff in das Grundrecht könne allenfalls die Verfolgung schwerer Straftaten sein. Gemessen am Prüfungsmaßstab dieser EuGH-Entscheidung standen daher auch die neu geschaffenen deutschen Regelungen in Frage, weshalb das Bundesverwaltungsgericht im Jahr 2019 die Entscheidung[55] getroffen hat, die Frage über die Rechtmäßigkeit des deutschen Gesetzes zur Vorratsdatenspeicherung an den EuGH abzugeben. Bis zu dessen Entscheidung bleibt eine Vorratsdatenspeicherung in Deutschland weiter ausgesetzt.

59 Das EU-Parlament hat Ende des Jahre 2009 eine Änderung der Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) beschlossen. Eine der elementaren Änderungen durch die sogenannte **Cookie-Richtlinie 2009/136/EG** betrifft die Speicherung bzw. den Zugriff auf Informationen auf Endgeräten der Nutzer – im Wesentlichen also die Verwendung von Cookies. Gem. Art. 2 Abs. 5 RL 2009/136/EG wurde Art. 5 der Datenschutzrichtlinie für elektronische Kommunikation dahingehend geändert, dass der Nutzer nun einwilligen musste, wenn Cookies verwendet werden sollten. Es erfolgte somit ein Wechsel vom „Opt-out-" zum „Opt-in-Prinzip".

60 Zuletzt wurden ebenso zeitgleich mit der Datenschutzgrundverordnung zwei weitere Richtlinien mit datenschutzrechtlichem Bezug verabschiedet. Das ist zum einen die **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. Die Richtlinie hat zum Ziel, den freien Verkehr personenbezogener Daten zwischen den zuständigen Behörden zum Zweck der Verhütung, Ermittlung oder Verfolgung von Straftaten oder der Strafvollstreckung zu erleichtern. Gleichzeitig soll dabei ein hohes Schutzniveau für die Verarbeitung von personenbezogenen Daten gewährleistet sein. Bei dem zweiten Rechtsakt handelt es sich um die **Richtlinie (EU) 2016/681** des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Ziel dieser Richtlinie ist es, durch die Verwendung und Speicherung von bestimmten Fluggastdaten – den sogenannten Passenger Name Record – für mehr Sicherheit zu sorgen und einen Beitrag im Kampf gegen den Terrorismus und schwerste Kriminalität zu leisten. Beide Richtlinien wurden am 4. Mai 2016 im

55 Pressemitteilung Bundesverwaltungsgericht Nr. 66/2019 vom 25. 09. 2019.

Amtsblatt der EU veröffentlich, traten am 25. Mai 2016 in Kraft[56] und wurden im Anschluss in nationales Recht[57] umgesetzt.

61 Die bisherigen Ausführungen machen bereits deutlich, dass die gesetzlichen Rahmenbedingungen für den Datenschutz in Deutschland stark von unionsrechtlichen Vorgaben geprägt sind. Der Schritt mit der wohl am weitest gehenden Tragweite für die Harmonisierung des Datenschutzes in Europa war aber mit der Verabschiedung der DSGVO getan. Die DSGVO hat auf Unionsebene das sogenannte „ordentliche Gesetzgebungsverfahren" (Art. 294 AEUV) durchlaufen. Die Gesetze starten dabei als ein Vorschlag der Kommission und werden dann vom Europäischen Parlament und vom Ministerrat über bis zu drei Lesungen gemeinsam angenommen.

62 Der Startschuss fiel am 25. Januar 2012, als die Kommission den Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)"[58] vorgelegt hat. Dieser wurde dem Europäischen Parlament und dem Ministerrat übermittelt. Am 12. März 2014 hat das Europäische Parlament zu diesem Vorschlag der Kommission Stellung genommen (Erste Lesung). Die Entschließung des Europäischen Parlamentes enthielt mehr als 200 Änderungsanträge gegenüber dem Vorschlag und wurde im Anschluss an den Ministerrat zu dessen Lesung übermittelt. Nachdem der Ministerrat aber nicht allen Änderungswünschen des Europäischen Parlamentes zustimmte, fasste er am 15. Juni 2015 seine Änderungswünsche im sogenannten „gemeinsamen Standpunkt" zusammen. Aus diesem Grund begannen am 24. Juni 2015 die sogenannten „Trilog-Verhandlungen". Hierbei handelt es sich um eine Abstimmung aller drei am Gesetzgebungsverfahren beteiligten Institutionen. Ziel war die Ausarbeitung eines gemeinsamen Entwurfes für die Datenschutz-Grundverordnung, der sowohl vom Europäischen Parlament, wie auch im Ministerrat in der „zweiten Lesung" angenommen wird. Am 15. Dezember 2015 schließlich haben sich die Verhandlungsführer der EU-Kommission, des EU-Parlaments sowie der Mitgliedstaaten auf einen Text für die Neuregelung des Datenschutzes geeinigt. Der Text wurde daraufhin in alle 22 Amtssprachen der EU übersetzt und konsolidiert. Nach der Billigung des Entwurfes im Europäischen Parlament und Ministerrat wurde die DSGVO am 4. Mai 2016 im Amtsblatt der Europäischen Union[59] veröffentlicht. Sie trat am 25. Mai 2016 in Kraft und wurde zum 25. Mai 2018 wirksam.

56 RL (EU) 2016/680 v. 27. 04. 2016 und RL (EU) 2016/681 v. 27. 04. 2016, ABl. 2016 Nr. L 119/1 v. 04. 05. 2016.

57 Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20. November 2019, BGBl. I S. 1724 sowie Gesetz zur Umsetzung der Richtlinie (EU) 2016/681 vom 6. Juni 2017, BGBl. I S. 1484.

58 Europäische Kommission v. 25. 01. 2012 – KOM (2012) 11 endgültig.

59 VO (EU) 2016/679 v. 27. 04. 2016, ABl. 2016 Nr. L 119/1 v. 04. 05. 2016.

Wie zuvor dargestellt genießt die DSGVO nach Art. 288 Abs. 2 AEUV als Verordnung unmittelbare Wirkung. Sie ist also ohne Umsetzungsakt unmittelbar in allen Mitgliedstaaten verbindliches Recht. Das nationale Recht wird durch die Verordnung jedoch nicht aufgehoben. Beide Rechtsordnungen stehen nebeneinander und beanspruchen weiterhin ihre Geltung.[60] Zwar haben die Mitgliedstaaten ihre Souveränität insoweit beschränkt, als dass sie der Europäischen Union Rechtssetzungskompetenzen übertragen haben, die auch für die Mitgliedstaaten verbindlich sind, jedoch beinhaltet dies keine Kompetenz die es ermöglichen könnte, nationale Gesetze außer Kraft zu setzen. Im Ergebnis gelten daher die deutschen Datenschutzgesetze neben der DSGVO weiter. Um einen Konflikt aus divergierenden Norminhalten zu vermeiden, genießt die DSGVO als europäische Verordnung aber **Anwendungsvorrang.**[61] Dieser Vorrang verpflichtet die innerstaatlichen Organe das unmittelbar geltende Unionsrecht ohne Rücksicht auf nationales Recht anzuwenden und entgegenstehendes innerstaatliches Recht unberücksichtigt zu lassen.[62] Am Beispiel des BDSG-alt hatte dies konkret zur Folge, dass diejenigen Teile des Gesetzes nicht mehr angewendet werden durften, für die die DSGVO eine abschließende Regelung beinhaltete. Im Ergebnis führte dies zu einer kaum zu durchschauenden Gemengelage von nationalem und europäischen Recht. Diese wurde zwar durch die Überarbeitung des BDSG in weiten Teilen aufgelöst, erfordert aber nach wie vor für einzelne nationale Gesetze mit datenschutzrechtlichem Bezug eine Einzelfallprüfung. 63

60 BVerfGE 22, 293 (296).
61 Schroeder, in: Streinz, EUV/AEUV, 2. Auflage 2012, Art. 288 AEUV, Rn. 40; Ruffert, in: Callies/Ruffert, EUV/AEUV, 5. Auflage 2016, Art. 288 AEUV, Rn. 20.
62 Herdegen, Europarecht, 18. Auflage 2016, § 10 Rn. 1.

2 Datenschutzrecht in Deutschland und in der EU

2.1 Maßgebliche Rechtsquellen

Ab dem 25. 05. 2018 sind die für Unternehmen maßgeblichen datenschutzrechtlichen Regelungen im Wesentlichen in diesen drei Gesetzen bzw. Verordnungen enthalten: 64

- Datenschutz-Grundverordnung (DSGVO)[1]
- Bundesdatenschutzgesetz (BDSG-neu)[2]
- E-Privacy-Verordnung (ePrivacy-VO, liegt im Entwurf vor)[3]

Die relevanten datenschutzrechtlichen Bestimmungen sind damit nicht mehr überwiegend im nationalen Recht zu finden. Maßgeblich sind vielmehr Vorschriften des europäischen Rechts. 65

2.1.1 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) – verabschiedet als VO (EU) 2016/679 – hat im Mai 2018 die Datenschutz-Richtlinie 95/46/EG abgelöst und das bis dahin geltende Bundesdatenschutzgesetz in weiten Teilen ersetzt. Sie entwickelt die aus den 90-er Jahren stammende Datenschutz-Richtlinie der Europäischen Union fort, ohne dabei mit den bekannten Grundsätzen und Systematiken zu brechen. Für Unternehmen in Deutschland, die mit den Regelungen und Begrifflichkeiten des Bundesdatenschutzgesetzes vertraut waren, bedeutete das Wirksamwerden der DSGVO daher keinen Umbruch. Dass dies in den Unternehmen mitunter anders wahrgenommen wurde, mag in dem Vollzugsdefizit datenschutzrechtlicher Vorschriften einerseits und den neuen Sanktionsmöglichkeiten der Aufsichtsbehörden begründet sein. 66

Auch wenn die Vorschriften der DSGVO im Wesentlichen nichts vollkommen Neues darstellen, so sind sie doch europäisches und nicht nationales Recht und sollten als solches wahrgenommen und angewandt werden. Für den Datenschutzbeauftragten in einem Unternehmen bedeutet dies, dass bei der Auslegung der Normen der DSGVO ein Blick in die Datenschutz-Richtlinie 95/46/EG hilfreicher sein wird als in das alte Bundesdatenschutzgesetz.[4] Rechtsanwender 67

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 04. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

2 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).

3 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 RL 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM (2017) 10 final.

4 Schantz, NJW 2016, 1841.

in Deutschland sollten nicht der Versuchung erliegen, die DSGVO als neue Fassung des Bundesdatenschutzgesetzes zu betrachten. Die DSGVO bietet in ihrer Anwendung in den Unternehmen die Chance, hergebrachte Grundsätze auf den Prüfstand zu stellen und ihre Fortgeltung unter der DSGVO zu überdenken.

68 Als Verordnung ist die DSGVO unmittelbar anwendbar. Anders als bei Richtlinien bedarf es keiner Umsetzung in nationales Recht.[5] Zwar sollte bereits die Datenschutz-Richtlinie 95/46/EG von 1995 zu einer Vollharmonisierung des Datenschutzrechts innerhalb der Europäischen Union führen.[6] Dieses Ziel wurde jedoch offenkundig nicht erreicht. Der Wechsel von dem Instrument der Richtlinie zur Verordnung war daher erforderlich, um in den Mitgliedstaaten der Europäischen Union ein weitgehend einheitliches Datenschutzniveau zu etablieren.

69 Inhaltlich ähnelt die DSGVO jedoch einer Richtlinie.[7] Sie enthält zahlreiche Öffnungs- und Spezifizierungsklauseln. Diese fordern den Gesetzgeber auf oder verpflichten ihn sogar, im nationalen Recht spezifische Regelungen zu treffen.

70 Die Mehrzahl der Öffnungs- und Spezifizierungsklauseln betrifft den Datenschutz im öffentlichen Bereich, also Behörden und andere öffentliche Stellen. Damit trägt die DSGVO den unterschiedlichen gesetzlichen Rahmenbedingungen in den Mitgliedstaaten der Europäischen Union Rechnung. Für Unternehmen sind nur wenige der Öffnungs- und Spezifizierungsklauseln von Bedeutung. Die für Unternehmen relevanten Öffnungs- und Spezifizierungsklauseln beschränken sich im Wesentlichen auf spezifische Vorschriften für den Beschäftigtendatenschutz und Videoüberwachung, die Einschränkung von Betroffenenrechten sowie ergänzende Bestimmungen zur verpflichtenden Benennung eines Datenschutzbeauftragten.

2.1.2 Bundesdatenschutzgesetz-neu

71 Der Deutsche Bundestag hat von den Öffnungs- und Spezifizierungsklauseln der DSGVO Gebrauch gemacht und am 27. 04. 2017 in dritter Lesung den Gesetzentwurf der Bundesregierung 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“) angenommen. Der Bundesrat stimmte dem Gesetz am 12. 05. 2017 zu, sodass das DSAnpUG-EU gemeinsam mit der DSGVO ab dem 25. 05. 2018 wirksam wurde. Wesentlicher Bestandteil des DSAnpUG-EU ist eine neue, an die DSGVO angepasste Fassung des Bundesdatenschutzgesetzes (BDSG-neu).

72 Damit bleibt den Rechtsanwendern in Deutschland der vertraute Name des Gesetzes erhalten. Systematisch kommt dem BDSG-neu jedoch eine vollkommen neue Rolle zu. Maßgeblich sind zunächst die Regelungen der DSGVO.

5 Dazu in Kapitel A 1.3.6.
6 EuGH, Urteil vom 24. 11. 2011 – C-468/10, C-469/10, C-468/10, C-469/10.
7 Kühling/Martini, EuZW 2016, 448, 449.

Soweit den Mitgliedstaaten dort durch Öffnungs- oder Spezifizierungsklauseln Konkretisierungen gestattet sind, müssen die Regelungen anwendbarer bereichsspezifischer Datenschutzvorschriften und – subsidiär – des BDSG-neu geprüft werden.[8]

2.1.3 ePrivacy-Verordnung

Neben den allgemeinen datenschutzrechtlichen Vorschriften der DSGVO enthält die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[9] („ePrivacy-Richtlinie") von 2002 bereichsspezifische Vorschriften für den Datenschutz in der Telekommunikation. Die Richtlinie wurde 2009 durch die so genannte Cookie-Richtlinie[10] ergänzt, die Regelungen für die Verwendung von Cookies und ähnlichen Technologien auf Webseiten enthält. 73

Ebenso wie die Datenschutz-Richtlinie 95/46/EG durch die DSGVO ersetzt wurde, soll die ePrivacy-Richtlinie durch eine neue ePrivacy-Verordnung (ePrivacy-VO) ersetzt werden. Diese soll die ePrivacy-Richtlinie fortentwickeln und die DSGVO im besonders datenschutzrelevanten Bereich der Telekommunikation um bereichsspezifische Datenschutzvorschriften ergänzen. 74

Im Januar 2017 hat die Europäische Kommission ihren Entwurf einer neuen ePrivacy-VO veröffentlicht. Formuliertes Ziel war, dass die ePrivacy-VO zeitgleich mit der DSGVO am 25. 05. 2018 wirksam wird.[11] Dieses Ziel wurde nicht erreicht. Über die Regelungen der ePrivacy-VO streiten die europäischen Institutionen noch heute. Im November 2020 hat der Rat der Europäischen Union einen neuen Entwurf veröffentlicht. Sobald die ePrivacy-VO Anwendung finden wird, werden für Unternehmen insbesondere die Vorgaben zur Reichweitenanalyse, zum Offline-Tracking sowie zur Verwendung von Cookies und ähnlichen Technologien von Bedeutung sein. Aufgrund ihres Anwendungsvorrangs wird die ePrivacy-VO die datenschutzrechtlichen Regelungen des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) verdrängen, sollten diese bis dahin noch in Kraft sein.[12] Mitte 2020 ist ein Entwurf für ein neues „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des TKG, des 75

8 Kühling, NJW 2017, 1985, 1987.
9 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. 07. 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.
10 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. 11. 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.
11 Siehe auch Kapitel A 1.3.6.
12 Engeler/Felber, ZD 2017, 251, 257.

TMG und weiterer Gesetze“[13] (TTDSG) öffentlich geworden. Der Bundestag hat das TTDSG am 20.05.2021 verabschiedet. Es wird zum 01.12.2021 in Kraft treten. Das TTDSG soll die durch das Nebeneinander von DSGVO, TMG und TKG bestehenden Rechtsunsicherheiten beseitigen, indem der Datenschutz und der Schutz der Privatsphäre in der Telekommunikation und bei Telemedien zukünftig einheitlich in einem Gesetz geregelt werden.

2.2 Grundlagen der Datenverarbeitung

2.2.1 Verbot mit Erlaubnisvorbehalt

76 Personenbezogene Daten dürfen gem. Art. 5 Abs. 1 lit. a DSGVO nur auf rechtmäßige Weise verarbeitet werden. Diese Vorgabe konkretisiert Art. 6 Abs. 1 DSGVO. Danach muss für die Rechtmäßigkeit einer Verarbeitung eine der dort geregelten Rechtsgrundlagen gegeben sein. In Art. 6 Abs. 1 DSGVO findet sich damit das aus § 4 Abs. 1 BDSG-alt bekannte Verbot mit Erlaubnisvorbehalt wieder.

77 Danach dürfen personenbezogene Daten nur verarbeitet werden, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat. Die wesentlichen Erlaubnistatbestände für Unternehmen sind:

- Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO)
- Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen (Art. 6 Abs. 1 S. 1 lit. b DSGVO)
- Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 S. 1 lit. c DSGVO)
- Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f DSGVO)

Einwilligung

78 Gemäß Art. 6 Abs. 1 S. 1 lit. a DSGVO stellt die Einwilligung eine Grundlage zur Verarbeitung personenbezogener Daten dar. Die Einwilligung ist in Art. 4 Abs. 8 DSGVO wie folgt definiert:

> *„Einwilligung der betroffenen Person (ist) jede ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“*

79 Die bisherige Definition in Art. 2 lit. h Datenschutz-Richtlinie lautet:

> *„Einwilligung der betroffenen Person (ist) jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.“*

13 Referentenentwurf des Bundesministeriums für Wirtschaft und Energie vom 14. 07. 2020 für ein Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze.

Zusätzlich verlangt Art. 7 lit. a Datenschutz-Richtlinie, dass die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben" hat.

Die Definition der Einwilligung in der DSGVO erhöht mit dem Merkmal **„unmissverständlich"** die Anforderungen an eine wirksame Einwilligung. Erforderlich ist nun eine eindeutige Erklärung oder Handlung der betroffenen Person. Die höheren Anforderungen einer ausdrücklichen Einwilligung sind nicht in die DSGVO übernommen worden. Eine ausdrückliche Einwilligung fordert die DSGVO nur in bestimmten Fällen. 80

Die Erteilung der Einwilligung erfordert eine **eindeutige Handlung.** Das kann eine schriftliche, elektronische oder mündliche Erklärung sein. Beispielhaft führt der Erwägungsgrund 25 das Anklicken eines Kästchens auf einer Webseite und die Auswahl technischer Einstellungen bei Online-Diensten auf. Keine Einwilligung stellen ein stillschweigendes Einverständnis, standardmäßig angekreuzte Kästchen oder Untätigkeit der betroffenen Person dar. 81

Sollen Daten für mehrere Zwecke verwendet werden, soll für jeden Verarbeitungszweck eine Einwilligung abgegeben werden (Erwägungsgrund 25). Erwägungsgrund 34 konkretisiert diese Anforderung und fordert, dass in verschiedene Datenverarbeitungsvorgänge jeweils gesondert eingewilligt werden kann. Andernfalls soll es an der Freiwilligkeit fehlen. 82

Vorformulierte Einwilligungen sollen gem. Art. 7 Abs. 2 DSGVO in einer klaren und einfachen Sprache zur Verfügung gestellt werden und dürfen keine missbräuchlichen Klauseln enthalten. Einwilligungserklärungen sollen zudem in verständlicher und leicht zugänglicher Form bereitgestellt werden. Zu diesen Punkten verweist Erwägungsgrund 32 auf die Richtlinie 93/13/EWG. Deren Art. 5 lautet: 83

> *„Sind alle dem Verbraucher in Verträgen unterbreiteten Klauseln oder einige dieser Klauseln schriftlich niedergelegt, so müssen sie stets klar und verständlich abgefasst sein. Bei Zweifeln über die Bedeutung einer Klausel gilt die für den Verbraucher günstigste Auslegung."*

Diese Themen sind nicht neu. Vorformulierte Einwilligungserklärungen unterzieht der BGH bereits seit Längerem der Inhaltskontrolle nach § 307 Abs. 1 BGB. Wird die Einwilligung im Zusammenhang mit anderen Erklärungen schriftlich abgegeben, ist sie **besonders hervorzuheben.** Diese Anforderung ist bereits aus § 4a Abs. 1 S. 4 BDSG-alt bekannt. 84

Die Einwilligung muss in Kenntnis der Sachlage abgegeben werden **(Transparenz).** Dazu sind der betroffenen Person mindestens Angaben zu dem Verantwortlichen und den Zwecken der Verarbeitung mitzuteilen. 85

Besonderes Augenmerk legt die DSGVO auf die **Freiwilligkeit.** Erwägungsgrund 32 fordert eine echte Wahlfreiheit und die Möglichkeit, die Einwilligung verweigern oder widerrufen zu können, ohne dadurch Nachteile befürchten zu müssen. Erwägungsgrund 34 ergänzt die Anforderungen an die Freiwilligkeit und erklärt die Einwilligung in Fällen eines klaren Ungleichgewichts zwischen betroffener Person und Verantwortlichem grundsätzlich für unwirksam. Dies 86

soll insbesondere für Behörden gelten, wird jedoch auch Auswirkungen auf die Einwilligung im Arbeitsverhältnis oder vergleichbare Konstellationen haben. Diese Auffassung vertreten die Aufsichtsbehörden bereits seit Längerem, wenngleich die Rechtsprechung des Bundesarbeitsgerichts mitunter eine andere Beurteilung erkennen und Raum für eine freiwillige Einwilligung im Arbeitsverhältnis lässt.

87 Das Recht der Mitgliedstaaten oder Betriebsvereinbarungen können Regelungen zur Verarbeitung von Beschäftigtendaten auf Grundlage einer Einwilligung vorsehen (Erwägungsgrund 124). Von dieser Möglichkeit hat der nationale Gesetzgeber in § 26 Abs. 2 BDSG-neu Gebrauch gemacht und die Anforderungen an eine Einwilligung im Beschäftigungsverhältnis konkretisiert.

88 Art. 7 Abs. 4 DSGVO in Verbindung mit Erwägungsgrund 34 untersagt, dass der Abschluss eines Vertrags von der Erteilung einer Einwilligung abhängig gemacht wird, obwohl dies für die Durchführung des Vertrags nicht erforderlich ist (Koppelungsverbot, kein „Take it or leave it"). Damit dehnt die DSGVO die aus § 28 Abs. 3b BDSG-alt bekannte Regelung deutlich aus. Danach war die Koppelung von Vertrag und (Werbe-)Einwilligung nur unzulässig, wenn der betroffenen Person ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.

89 Die **Verarbeitung besonderer Kategorien personenbezogener Daten** unterliegt nach Art. 9 DSGVO einem grundsätzlichen Verarbeitungsverbot. Eine Ausnahme hiervon gilt gem. Art. 9 Abs. 2 lit. a DSGVO unter anderem, wenn die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat. Diese Formulierung findet sich in ähnlicher Weise in § 4a Abs. 3 BDSG-alt.

90 Art. 7 Abs. 3 DSGVO sieht vor, dass die betroffene Person ihre Einwilligung jederzeit **widerrufen** kann. Auf dieses Recht ist die betroffene Person bei der Datenerhebung hinzuweisen (Art. 13 Abs. 2 lit. c DSGVO). Gründe müssen für den Widerruf nicht angegeben werden. Der Widerruf muss so einfach wie die Erteilung der Einwilligung möglich sein. Dieser Punkt ist wichtig bei der Gestaltung von Webseiten, Apps und anderen digitalen Diensten. Er erfordert im Regelfall die Bereitstellung einer Widerrufsmöglichkeit in demselben Kanal, in dem die Einwilligung abgegeben wurde.

91 Gegenüber dem bisherigen Recht stellt die freie Widerrufbarkeit der Einwilligung eine Verschärfung dar. Für den Widerruf der Einwilligung im Arbeitsverhältnis forderte das Bundesarbeitsgericht bisher z. B. einen plausiblen Grund.[14] Es sollte daher genau geprüft werden, welche Geschäftsprozesse zukünftig auf eine Einwilligung gestützt werden sollen. Es erscheint ratsam, wo immer möglich auf gesetzliche Erlaubnistatbestände, insbesondere die Interessenabwägung als Rechtsgrundlage zurückzugreifen.

92 Klarstellend enthält Art. 7 Abs. 3 DSGVO den Hinweis, dass der Widerruf der Einwilligung die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung

14 BAG, Urteil vom 19. 02. 2015 – 8 AZR 1011/13.

nicht berührt. Der Widerruf wirkt folglich nur ex nunc. Widerruft die betroffene Person ihre Einwilligung, sind ihre personenbezogenen Daten auf Verlangen zu löschen (Art. 17 Abs. 1 lit. b DSGVO). Sind die Daten an andere Stellen weitergegeben worden, muss der Verantwortliche die Empfänger über die Löschung informieren (Art. 19 DSGVO).

Dem Verantwortlichen obliegt gem. Art. 7 Abs. 1 DSGVO die **Beweislast** für das Vorliegen und die Reichweite der Einwilligung (siehe auch Erwägungsgrund 32). 93

Einwilligungserklärungen, die gegen die Vorgaben der DSGVO verstoßen, sind unwirksam (Art. 7 Abs. 2 S. 2 DSGVO). Dies kann auch nur für bestimmte Teile einer Einwilligungserklärung gelten. **Verstöße** gegen die Regelungen in Art. 6, 7 und 9 DSGVO einschließlich der Bedingungen für die Einwilligung können mit einer Geldbuße von bis zu 20 Millionen Euro oder von bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens geahndet werden (Art. 83 Abs. 5 lit. a DSGVO). Anders als noch § 43 Abs. 2 Nr. 1 BDSG-alt gilt die Bußgeldvorschrift erstmals auch ausdrücklich für die Umstände der Erteilung einer Einwilligung. 94

Bei Datenverarbeitungen auf Grundlage einer Einwilligung muss die betroffene Person mit Anwendbarkeit der DSGVO nicht erneut einwilligen, wenn die bereits erteilte Einwilligung den Bedingungen der DSGVO entspricht (Erwägungsgrund 134). Im Umkehrschluss bedeutet dies, dass Einwilligungen, die nicht den (strengeren) Kriterien der DSGVO entsprechen, erneut durch die betroffenen Personen zu erteilen sind. 95

Art. 8 DSGVO enthält besondere Vorgaben für die **Verarbeitung personenbezogener Daten eines Kindes.** Die Vorgaben sind nur bei einem Angebot von Diensten der Informationsgesellschaft (im Wesentlichen Online-Dienste) von Bedeutung, welches unmittelbar an das Kind adressiert ist. Soll die Verarbeitung auf Grundlage einer Einwilligung erfolgen, muss diese entweder durch die Eltern für das Kind oder mit deren Zustimmung durch das Kind abgegeben werden. Die Altersgrenze zieht die DSGVO grundsätzlich bei 16 Jahren. Die Mitgliedstaaten können niedrigere Altersgrenzen vorsehen (bis maximal 13 Jahren). Der Verantwortliche muss gem. Art. 8 Abs. 2 DSGVO durch angemessene Anstrengungen sicherstellen, dass die Einwilligung tatsächlich durch die Eltern abgegeben wurde. 96

In der Praxis sollten Unternehmen diesen Punkten besondere Beachtung schenken, wenn sie personenbezogene Daten auf Basis einer Einwilligung verarbeiten wollen: 97

– Opt-out-Einwilligungen, wie noch in dem PAYBACK-Urteil des BGH[15] gestattet, werden nicht mehr möglich sein. Notwendig ist nun stets eine eindeutige Handlung der betroffenen Person.

15 BGH, Urteil vom 16. 07. 2008 – VIII ZR 348/06.

- Die Formerfordernisse nach § 4a BDSG-alt und § 13 Abs. 2 TMG entfallen und werden harmonisiert. Art. 7 DSGVO verlangt keine Schriftform. Möglich sind schriftliche, elektronische oder mündliche Erklärungen.
- Hinsichtlich für die Vertragsdurchführung nicht notwendiger Daten wird die Einwilligung deutlich erschwert. Dies gilt auch bei einem klaren Ungleichgewicht der Vertragspartner.
- Das Koppelungsverbot verbietet für den Regelfall den bei dem Angebot von Online-Diensten bekannten „Take it or leave it"-Ansatz.
- Die Einbindung von Einwilligungserklärungen in Allgemeine Geschäftsbedingungen wird schwieriger.
- Bei der Verarbeitung personenbezogener Daten eines Kindes gelten Besonderheiten.
- Die freie Widerrufbarkeit der Einwilligung schafft Rechtsunsicherheit bei Geschäftsprozessen, die auf eine verlässliche rechtliche Grundlage angewiesen sind.

Gesetzliche Erlaubnistatbestände

98 Die wichtigsten gesetzlichen Erlaubnistatbestände für Unternehmen wurden bereits oben aufgeführt. Hier noch einmal kurz zur Wiederholung:

- Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen (Art. 6 Abs. 1 S. 1 lit. b DSGVO)
- Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 S. 1 lit. c DSGVO)
- Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f DSGVO)

99 Gemäß Art. 6 Abs. 1 lit. b DSGVO dürfen personenbezogene Daten verarbeitet werden, wenn dies zur **Erfüllung eines Vertrages** oder zur **Durchführung vorvertraglicher Maßnahmen** erforderlich ist. Vertrag ist dabei jedes rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnis.[16] Auch vertragsähnliche Verhältnisse sind von dieser Regelung erfasst.[17] Dritte, die an dem Vertragsverhältnis nicht unmittelbar beteiligt sind, können sich ebenfalls auf den Erlaubnistatbestand stützen, solange die Verarbeitung für die Vertragserfüllung erforderlich und die betroffene Person Partei dieses Vertrags ist. Vorvertragliche Maßnahmen im Stadium der Vertragsanbahnung (dazu gehören insbesondere Vertragsverhandlungen) sind auf Basis von Art. 6 Abs. 1 lit. b DSGVO ebenfalls legitimiert. Voraussetzung dafür ist, dass sie auf Initiative der betroffenen Person erfolgen. Begrenzt wird die Verarbeitung zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen durch das Kriterium der Erforderlichkeit. Erforderlich sind in jedem Fall Verarbeitungen, ohne die der Vertrag nicht durchgeführt werden könnte, wie z. B. die Verwendung der Lieferadresse für die Zustellung einer online aufgegebenen Bestellung. Im Übrigen bedarf es

16 Albers, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 08. 2017, Art. 6 Rn. 30.

17 Albers, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 08. 2017, Art. 6 Rn. 30.

für die Bestimmung der Erforderlichkeit einer Analyse der konkret vereinbarten Vertragsklauseln und den darin geregelten vertraglichen Rechten und Pflichten.[18] Die Bestimmung der Erforderlichkeit anhand eines abstrakt-wertenden Maßstabs, wie unter anderem von dem Europäischen Datenschutzausschluss vertreten, ist abzulehnen.[19]

Gemäß Art. 6 Abs. 1 lit. c DSGVO dürfen personenbezogene Daten verarbeitet werden, wenn dies zur **Erfüllung der dem Verantwortlichen obliegenden rechtlichen Verpflichtungen** erforderlich ist. Die rechtliche Verpflichtung muss sich gem. Art. 6 Abs. 3 DSGVO aus dem Unionsrecht oder dem Recht eines Mitgliedstaates ergeben. Für Unternehmen sind in diesem Zusammenhang z. B. die sich aus dem Handels- und Steuerrecht ergebenden Aufbewahrungspflichten von Bedeutung. 100

Gemäß Art. 6 Abs. 1 lit. f DSGVO dürfen personenbezogene Daten verarbeitet werden, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dem Erlaubnistatbestand der **Interessenabwägung** kommt eine zentrale Bedeutung für die Legitimierung von Verarbeitungen personenbezogener Daten durch Unternehmen zu. Der Interessenabwägung obliegt es, die berechtigten Verarbeitungsinteressen von Unternehmen mit den schutzwürdigen Interessen der betroffenen Personen in Einklang zu bringen. 101

Berechtigt ist jedes legitime rechtliche, wirtschaftliche oder ideelle Interesse des Verantwortlichen.[20] Erwägungsgründe 47, 48 und 49 nennen beispielhaft Betrugsprävention, Direktwerbung, Maßnahmen zur Verbesserung der Sicherheit von IT-Systemen sowie das Interesse einer Unternehmensgruppe, Daten zu internen Verwaltungszwecken auszutauschen. Bei der Bestimmung der berechtigten Interessen sind nach Erwägungsgrund 47 die **vernünftigen Erwartungen der betroffenen Person** zu berücksichtigen. Diese beruhen ihrerseits auf der Beziehung der betroffenen Person zu dem Verantwortlichen sowie auf der Vorhersehbarkeit einer Verarbeitung. Dabei kann der Verantwortliche versuchen, die Vorhersehbarkeit über die Informationen, welche er der betroffenen Person über die von ihm beabsichtigten Verarbeitungen zur Verfügung stellt, ein Stück weit zu steuern. 102

18 Engeler, NJW 2018, 55, 57.

19 Europäischer Datenschutzausschuss, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0 vom 08. 10. 2019; Engeler, NJW 2018, 55, 57.

20 Albers/Veit, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, Art. 6 Rn. 49.

2.2.2 Personenbezogene Daten

103 Die gesetzlichen Bestimmungen zum Datenschutz kommen nur zur Anwendung, wenn personenbezogene Daten verarbeitet werden. Dem Begriff des personenbezogenen Datums kommt im Datenschutzrecht damit entscheidende Bedeutung zu. Weil das Vorliegen von personenbezogenen Daten Voraussetzung für die Anwendbarkeit der datenschutzrechtlichen Vorschriften ist, besteht über die Auslegung des Begriffs seit jeher Streit. In Erinnerung gerufen sei an dieser Stelle nur der Streit über den Personenbezug von dynamischen IP-Adressen und die in dieser Sache erfolgte Entscheidung durch den Europäischen Gerichtshof im Oktober 2016.[21]

104 Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen".*

Damit enthält die DSGVO für den Begriff des personenbezogenen Datums eine ähnliche Definition wie sie zuvor in § 3 Abs. 1 BDSG-alt verwendet wurde. Danach waren personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person".

105 Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann. Die Identifizierung kann insbesondere über die Zuordnung zu einer Kennung erfolgen. Primäres Identifizierungsmerkmal ist der Name einer Person. Aber eine Person kann auch über eine Kennnummer (z. B. Steueridentifikationsnummer, Sozialversicherungsnummer) oder Online-Kennung (z. B. Benutzername, IP-Adresse, Cookie-ID, Apple-IDFA, Google-Werbe-ID), mithilfe von Standortdaten oder über eine Zuordnung zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der Person sind, identifiziert werden. Für die Identifizierbarkeit einer Person kommt es nicht darauf an, ob die Person namentlich bekannt ist.[22] Entscheidend ist, dass die Daten ein Wiedererkennen der Person (singling out) und damit eine Unterscheidung von anderen Personen ermöglichen.[23]

106 Der Verantwortliche muss bei der Prüfung, ob eine Person identifizierbar ist, alle Mittel berücksichtigen, deren Nutzung für die Identifizierung der Person objektiv wahrscheinlich ist. Die entscheidende Frage in diesem Zusammenhang ist, wessen Fähigkeiten, Mittel und Wissen maßgeblich sind, um zu beurteilen, ob ein Personenbezug herstellbar ist. Kommt es auf die Erkenntnismöglichkeiten des Verantwortlichen (relativer Personenbezug) an oder muss der Verant-

21 EuGH, Urteil vom 19. 10. 2016 – C-582/14 (Breyer/Deutschland).
22 Artikel 29-Datenschutzgruppe, WP 136 vom 20. 06. 2007, S. 14.
23 Schild, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 11. 2020, Art. 4 Rn. 17.

wortliche das Wissen Dritter einbeziehen, selbst wenn er darauf nicht ohne Weiteres zugreifen kann (absoluter Personenbezug)?

Die DSGVO beantwortet diese Frage, wie bereits zuvor die Datenschutz-Richtlinie 95/46/EG, nicht eindeutig. Erwägungsgrund 26 enthält insoweit lediglich den Hinweis, dass allein die Mittel maßgeblich sind, die der Verantwortliche nach allgemeinem Ermessen wahrscheinlich einsetzen wird, um eine Person zu identifizieren. Dies spricht für einen gemischt absolut-relativen Ansatz für die Bestimmung des Personenbezugs. 107

Wegen der dargestellten Unterschiede in der Auslegung der Identifizierbarkeit einer betroffenen Person ist es für den Rechtsanwender mitunter schwierig zu bestimmen, ob ein Datum Personenbezug aufweist oder nicht. Zwar ist die Mehrzahl der Fälle eindeutig zuzuordnen. In der Praxis immer häufiger sind jedoch Fälle, in denen nicht mit Sicherheit gesagt werden kann, ob ein Datum personenbezogen oder vielmehr vollständig anonym ist. Grund hierfür sind die unter den Bedingungen der Digitalisierung zahlreichen Möglichkeiten, gespeicherte Daten mit anderen Datenbeständen zu verknüpfen oder aus vorhandenen Daten neue Erkenntnisse abzuleiten, die wiederum einen Rückschluss auf eine natürliche Person zulassen. 108

Beispielhaft sei hier das Tracken von Personen im öffentlichen Raum (genauer: das Tracken des von einer Person bei sich geführten mobilen Endgeräts) anhand der von dem mobilen Endgerät ausgesendeten MAC-Adresse genannt. Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse eines Netzwerkadapters. Sie dient dazu, ein Gerät in einem Netzwerk eindeutig zu identifizieren. Für sich genommen identifiziert die MAC-Adresse damit zunächst lediglich ein Gerät. Die Person, welche das Gerät nutzt, kann ohne Zusatzinformationen nicht bestimmt werden. Werden jedoch unter der MAC-Adresse oder einem Pseudonym, welches die MAC-Adresse ersetzt, die Bewegungen einer Person in einem Raum für eine bestimmte Zeit aufgezeichnet, können die so erhobenen Daten einen Personenbezug aufweisen.[24] Dazu muss die das Gerät nutzende Person nicht zwingend namentlich bekannt sein. Ausreichend ist, wenn die Person in den erhobenen Daten aufgrund ihres Nutzungsverhaltens eindeutig identifiziert werden kann (singling out). Zur Vermeidung rechtlicher Unsicherheiten sollte der Begriff des personenbezogenen Datums daher weit ausgelegt und im Zweifel von dem Vorliegen personenbezogener Daten ausgegangen werden. 109

Dies gilt vor allem für die Praxis. Insbesondere wenn eine Verarbeitung darauf angelegt ist, eine Identifizierung der betroffenen Person zu ermöglichen (sei es als Kunde, Mitarbeiter oder in einer sonstigen Rolle), sollte daher davon ausgegangen werden, dass personenbezogene Daten vorliegen. Bei anonymen Daten finden die datenschutzrechtlichen Vorschriften hingegen keine Anwendung. 110

24 Conseil d'État, Urteil vom 08. 02. 2017, Nr. 393714, https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000034017907 (letzter Abruf: 09. 11. 2020).

Tatsächliche Anonymität von Daten, wie sie die datenschutzrechtlichen Vorschriften fordern, ist in der Praxis jedoch nur schwer zu erreichen.

2.2.3 Besondere Kategorien von personenbezogenen Daten

111 Art. 9 DSGVO stellt besondere Kategorien von personenbezogenen Daten unter besonderen Schutz. Im Einzelnen sind dies:

- Daten über die rassische und ethnische Herkunft;
- Daten über politische Meinungen, religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftszugehörigkeit;
- genetische Daten;
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person;
- Gesundheitsdaten;
- Daten zum Sexualleben oder der sexuellen Orientierung.

Der Katalog der besonders geschützten Datenarten ist weitgehend aus dem Bundesdatenschutzgesetz bekannt. Die DSGVO ergänzt den Katalog um weitere Kategorien besonders schutzbedürftiger Daten (genetische und biometrische Daten).

112 Für besondere Kategorien personenbezogener Daten besteht gem. Art. 9 Abs. 1 DSGVO ein grundsätzliches **Verarbeitungsverbot.** Nur bei Vorliegen der in Art. 9 Abs. 2 DSGVO beschriebenen Voraussetzungen kommt eine Verarbeitung besonderer Kategorien personenbezogener Daten in Betracht.

113 Keine besonderen Kategorien personenbezogener Daten sind **Daten über strafrechtliche Verurteilungen und Straftaten** oder damit zusammenhängende Sicherungsmaßregeln. Diese genießen jedoch ebenfalls einen besonderen Schutz und dürfen nur unter den besonderen Voraussetzungen von Art. 10 DSGVO verarbeitet werden.

2.2.4 Besondere Verarbeitungssituationen

114 In den §§ 26 bis 31 BDSG-neu sind Regelungen für besondere Verarbeitungssituationen enthalten. Für Unternehmen sind insbesondere die in § 26 BDSG-neu enthaltenen Bestimmungen über den Beschäftigtendatenschutz von Bedeutung, welche der nationale Gesetzgeber aufgrund der in Art. 88 DSGVO enthaltenen Öffnungs- und Spezifizierungsklausel erlassen durfte.

115 § 26 BDSG-neu schreibt im Wesentlichen die Grundsätze des § 32 BDSG-alt fort.[25] Bestrebungen für ein umfassendes Beschäftigtendatenschutzgesetz haben keinen Eingang in das BDSG-neu gefunden.

116 Weiterhin relevant ist für Unternehmen § 31 BDSG-neu, der das Scoring und die Erteilung von Bonitätsauskünften durch Auskunfteien regelt. Die Vorschrift

25 BT-Drs. 18/11325, S. 96 f.

verfolgt erkennbar das Ziel, das Schutzniveau der bisherigen §§ 28a, 28b BDSG-alt beizubehalten.

2.3 Datenschutzrechtliche Grundsätze

Art. 5 DSGVO enthält die Grundsätze der Verordnung. Diese beruhen auf den Vorgaben von Art. 8 Abs. 2 der Charta der Grundrechte der Europäischen Union (GRCh). Für den Anwender der DSGVO ist es von besonderer Wichtigkeit, sich mit den in Art. 5 DSGVO enthaltenen Grundsätzen vertraut zu machen. Zum einen sind die datenschutzrechtlichen Grundsätze **für die Auslegung** der zahlreich in der Verordnung enthaltenen unbestimmten Rechtsbegriffe **von maßgeblicher Bedeutung.** Zum anderen können Verstöße von den Aufsichtsbehörden mit einem Bußgeld von bis zu vier Prozent des weltweit erzielten Jahresumsatzes geahndet werden. 117

Jede Verarbeitung personenbezogener Daten muss die in Art. 5 DSGVO normierten Datenschutzgrundsätze erfüllen. Anders als z. B. noch die Regelungen zur Datenvermeidung und Datensparsamkeit in § 3a BDSG, gehen die Grundsätze der Verordnung damit über im Ergebnis folgenlose Programmsätze hinaus. Sie stellen vielmehr **verbindliche Regelungen** dar, die durch den Verantwortlichen unmittelbar zu beachten sind. Die Verordnung unterstreicht dies mit der Einführung des neuen Grundsatzes der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO. Danach wird dem Verantwortlichen die Einhaltung der Datenschutzgrundsätze aufgegeben und die jederzeitige Nachweisbarkeit verlangt. 118

2.3.1 Rechtmäßigkeit

Der in Art. 5 Abs. 1 lit. a DSGVO enthaltene Grundsatz der Rechtmäßigkeit entspricht dem aus § 4 Abs. 1 BDSG-alt bekannten **Verbot mit Erlaubnisvorbehalt.** Art. 6 Abs. 1 DSGVO konkretisiert diesen Grundsatz. Auch nach der DSGVO ist eine Verarbeitung personenbezogener Daten damit nur gestattet, wenn die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat oder eine gesetzliche Vorschrift die Verarbeitung erlaubt. Die wichtigsten gesetzlichen Erlaubnistatbestände stellen für Unternehmen neben der Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), die Verarbeitung zur Durchführung eines Vertrags mit der betroffenen Person (Art. 6 Abs. 1 lit. b DSGVO) und die Verarbeitung aufgrund einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) dar. 119

2.3.2 Treu und Glauben

Art. 5 Abs. 1 lit. a DSGVO legt weiter fest, dass personenbezogene Daten nach Treu und Glauben zu verarbeiten sind. Der deutsche Rechtsanwender mag in diesem Zusammenhang an den in § 242 BGB verankerten zivilrechtlichen Grundsatz von Treu und Glauben denken. Diese Bedeutung kommt dem datenschutzrechtlichen Grundsatz von Treu und Glauben jedoch nicht zu. 120

Der Ansatz ist ein anderer. Klarer wird die Bedeutung des Grundsatzes von Treu und Glauben bei Hinzuziehung der englischen Fassung der DSGVO. Diese be- 121

zeichnet den Grundsatz von Treu und Glauben mit dem Begriff **„Fairness".** Das erscheint für die Rechtsanwendung der passendere Begriff zu sein und bietet zugleich Orientierung für die nähere Bestimmung des Begriffs.

122 Eine „faire" Datenverarbeitung lässt sich als Ausprägung des **Verhältnismäßigkeitsgrundsatzes** verstehen. Die Verarbeitung personenbezogener Daten muss also zur Erreichung eines legitimen Zwecks geeignet, erforderlich und angemessen sein. „Fair" ist eine Datenverarbeitung zudem, wenn die Daten unmittelbar bei der betroffenen Person erhoben werden. So kann die betroffene Person in der Regel erkennen und nachvollziehen, welche Daten von wem für welche Zwecke verarbeitet werden sollen. Dem Grundsatz von Treu und Glauben lässt sich insoweit ein **Vorrang der Direkterhebung** entnehmen.[26] Er weist zudem enge Bezüge zu dem Grundsatz der Transparenz auf.

2.3.3 Transparenz

123 Der Grundsatz der Transparenz (ebenfalls verankert in Art. 5 Abs. 1 lit. a DSGVO) fordert den Verantwortlichen auf, personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise zu verarbeiten. Erwägungsgrund 39 lässt sich entnehmen, dass die betroffene Person zumindest Informationen über die Identität des Verantwortlichen, die Zwecke der Verarbeitung sowie sonstige Informationen zur Gewährleistung einer fairen und transparenten Verarbeitung erhalten soll. Dabei wirkt das Prinzip der Transparenz nicht nur retrospektiv, sondern auch prospektiv.[27] Die betroffene Person muss die Datenverarbeitung demnach für die Vergangenheit nachvollziehen und zumindest in ihren wesentlichen Aspekten für die Zukunft vorhersehen können.

124 Der Grundsatz der Transparenz erfährt in den Art. 12 ff. DSGVO umfangreiche Konkretisierungen. Von besonderer Bedeutung sind für Unternehmen die in Art. 13 und 14 DSGVO geregelten Informationspflichten sowie der in Art. 15 DSGVO enthaltene Auskunftsanspruch. In der Gesamtschau der Regelungen erhebt die DSGVO Transparenz damit zu einem ihrer **wesentlichen Prinzipien.**

2.3.4 Zweckbindung

125 Art. 5 Abs. 1 lit. b DSGVO regelt den Kern des Datenschutzrechts. Er bestimmt, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden (Grundsatz der Zweckfestlegung und -bindung). Kern des Datenschutzrechts ist dieser Grundsatz, weil der Zweck einer Datenverarbeitung der Maßstab für die Beurteilung wesentlicher Fragen im Zusammenhang mit der Zulässigkeit einer Datenverarbeitung ist. So gibt der Zweck die **Erforderlichkeit** der Verarbeitung mit Blick auf Art und Umfang der erhobenen Daten vor, bestimmt die **Rechtsgrundlage** gem. Art. 6 Abs. 1 DSGVO und legt den

26 Schantz, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, Art. 5 Rn. 9.

27 Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 3. Auflage 2021, Art. 5 Rn. 21.

Umfang der nach Art. 13 und 14 DSGVO bestehenden **Informationspflichten** sowie die nach Art. 17 DSGVO bestehenden **Löschfristen** fest.

Wegen dieser herausragenden Bedeutung ist der von dem Verantwortlichen verfolgte Zweck **vor Beginn der Verarbeitung** festzulegen.[28] Mit Blick auf die in der DSGVO enthaltenen Dokumentations- und Nachweispflichten empfiehlt es sich in der Praxis, den Zweck schriftlich oder in einem elektronischen Format zu dokumentieren. Die Dokumentation sollte so erfolgen, dass der Verantwortliche jederzeit in der Lage ist, den Zweck einer Verarbeitung nachzuweisen – sei es gegenüber der Aufsichtsbehörde oder gegenüber der betroffenen Person im Fall eines Auskunftsersuchens. Mit der schriftlichen und damit nachvollziehbaren Festlegung des Verarbeitungszwecks erfüllt der Verantwortliche gleichzeitig einen wichtigen Baustein der ihn gem. Art. 5 Abs. 2 DSGVO treffenden Rechenschaftspflicht. 126

Eine in der Praxis wichtige Frage ist, wie **detailliert** der Zweck von dem Verantwortlichen zu beschreiben ist. Dies ist zum einen für die Gestaltung von Datenschutzerklärungen relevant. In dieser beschreibt der Verantwortliche, für welche Zwecke er die personenbezogenen Daten der betroffenen Person verarbeiten will. Damit kommt er den in Art. 13, 14 DSGVO enthaltenen Informationspflichten nach. Zugleich kommt er damit seiner Pflicht zur Festlegung des Verarbeitungszwecks nach. Zum anderen ist die Frage, wie detailliert der Zweck von dem Verantwortlichen zu beschreiben ist, für die Frage einer Zweckänderung von Bedeutung. Je detaillierter der Zweck einer Datenverarbeitung festgelegt ist, desto eher ist bei einer Weiterverarbeitung eine Zweckänderung gegeben. Eine Verarbeitung für einen anderen als den ursprünglich festgelegten Zweck ist nur unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO zulässig. 127

Dem Wortlaut von Art. 5 Abs. 1 lit. b DSGVO lässt sich entnehmen, dass es sich um „eindeutige" Zwecke handeln muss. Eindeutig ist ein Zweck nur, wenn die betroffene Person ohne Weiteres erkennen kann, welches Ziel der Verantwortliche bei der Verarbeitung verfolgt und auf welche Weise dieses Ziel erreicht werden soll. Generelle Beschreibungen des Verarbeitungszwecks, wie z. B. „Verbesserung der Benutzerfreundlichkeit" oder „Marketing", sind daher nicht ausreichend, um das Gebot der eindeutigen Festlegung des Verarbeitungszwecks zu erfüllen.[29] Bei Verwendung derart genereller Zweckbeschreibungen kann die betroffene Person nicht erkennen, welche Verarbeitung ihrer Daten von dem angegebenen Zweck umfasst ist und welche nicht. 128

Die Beantwortung der Frage, wie detailliert der Verarbeitungszweck von dem Verantwortlichen zu beschreiben ist, hängt im Ergebnis von den konkreten Umständen der Datenerhebung sowie Art und Umfang der verarbeiteten Daten ab. Beispiel: Werden auf einer Gewinnspielkarte Name und Anschrift des Teilnehmers abgefragt und sollen diese Daten ausschließlich für die Durchführung des Gewinnspiels einschließlich der Benachrichtigung des Gewinners verwen- 129

28 Artikel 29-Datenschutzgruppe, WP 203 vom 02. 04. 2013, S. 15.
29 Artikel 29-Datenschutzgruppe, WP 203 vom 02. 04. 2013, S. 16.

det werden, reicht es aus, dies in einem kurzen Datenschutzhinweis auf der Gewinnspielkarte zu vermerken. Für den Teilnehmer ist der Verwendungszweck seiner Daten ohne Weiteres ersichtlich. Ist die Veranstaltung des Gewinnspiels jedoch Bestandteil eines Kundenbindungssystems und sollen die erhobenen Daten zu bereits vorhandenen Daten hinzugespeichert und die so zusammengeführten Daten für Zwecke der personalisierten Werbung verwendet werden, bedarf es einer ausführlicheren Angabe des Verarbeitungszwecks. Diese muss den Teilnehmer in die Lage versetzen, die Verarbeitung seiner Daten nachzuvollziehen.

2.3.5 Datenminimierung

130 Art. 5 Abs. 1 lit. c DSGVO enthält den Grundsatz der Datenminimierung. Danach müssen personenbezogene Daten, welche der Verantwortliche erhebt, dem Zweck angemessen und erheblich sowie auf das für die Verarbeitungszwecke notwendige Maß beschränkt sein. Der Grundsatz der Datenminimierung umfasst damit drei unterschiedliche Elemente. Diese entsprechen im Kern einer Verhältnismäßigkeitsprüfung mit den Aspekten Geeignetheit („für den Zweck erheblich"), Erforderlichkeit („auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt") und Angemessenheit („dem Zweck angemessen").

131 Ausgangspunkt der Betrachtung ist dabei der Zweck der Verarbeitung. Die Daten müssen den von dem Verantwortlichen verfolgten Zweck zu fördern in der Lage sein. Nur dann sind sie für den Zweck erheblich. Daten, die für den angestrebten Zweck nicht benötigt werden, dürfen gemäß dem Grundsatz der Datenminimierung nicht erhoben werden.

132 Der Verantwortliche darf nur die Daten verarbeiten, die zur Erreichung des verfolgten Zwecks erforderlich sind. Damit begrenzt der Grundsatz der Datenminimierung Art und Umfang der Datenerhebung durch den Verantwortlichen je nachdem, in welchem Zusammenhang die Daten erhoben und für welche Zwecke sie verwendet werden sollen. Klassisches Beispiel ist die Bestellung eines Newsletters. Erforderlich ist allein die Angabe der E-Mail-Adresse für den Empfang des Newsletters. Die Angabe weiterer Daten, wie z. B. der Name des Empfängers für eine persönliche Ansprache, mag aus Sicht des Verantwortlichen sinnvoll sein, ist für die Zustellung des Newsletters aber nicht notwendig. Das Element der Erforderlichkeit als Bestandteil des Grundsatzes der Datenminimierung ist bereits in den Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO enthalten. Die dort geregelte Erforderlichkeit ist mit dem Prinzip der Erforderlichkeit als Element des Grundsatzes der Datenminimierung inhaltlich deckungsgleich.

133 Ein normatives Mehr lässt sich der Angemessenheit der Verarbeitung als drittem Aspekt des Grundsatzes der Datenminimierung entnehmen. Die Angemes-

senheit erfordert eine wertende Betrachtung der Verarbeitung und soll eine Verarbeitung im Übermaß mit Blick auf den verfolgten Zweck unterbinden.[30]

2.3.6 Richtigkeit

Die DSGVO verlangt von dem Verantwortlichen, dass die von ihm verarbeiteten Daten richtig sind und, soweit dies für die Verarbeitung erforderlich ist, aktualisiert werden. Dieser Grundsatz enthält für den Verantwortlichen damit die Pflicht zur Umsetzung geeigneter Maßnahmen, um unrichtige Daten zu löschen oder zu berichtigen. In der Praxis hat der schon aus der Datenschutz-Richtlinie 95/46/EG bekannte Grundsatz keine besondere Beachtung gefunden. Ein Grund hierfür ist, dass der Grundsatz – mit Ausnahme der in § 35 Abs. 1 S. 1 BDSG-alt enthaltenen Aufforderung an den Verantwortlichen, unrichtig gespeicherte personenbezogene Daten zu berichtigen – keine explizite Umsetzung im BDSG-alt gefunden hat. 134

Zur Verwirklichung des Grundsatzes der Richtigkeit hat der Verantwortliche angemessene Maßnahmen zu treffen. Entscheidendes Kriterium ist dabei das in Art. 5 Abs. 1 lit. d DSGVO formulierte Gebot, dass die Richtigkeit im Hinblick auf die Zwecke ihrer Verarbeitung sichergestellt sein muss.[31] Dies bedeutet, dass bei der Verarbeitung von Bonitätsdaten zur Übermittlung an Dritte durch eine Auskunftei höhere Anforderungen an die Richtigkeit der Daten zu stellen sind, als bei der Verarbeitung von Daten für Zwecke der Werbung oder Marktforschung. Bei der Auswahl der Maßnahmen zur Gewährleistung der Richtigkeit der Daten, sollte der Verantwortliche folglich insbesondere die potenziellen Folgen für die betroffene Person berücksichtigen, die mit der Verarbeitung unrichtiger Daten verbunden sein können. 135

2.3.7 Speicherbegrenzung

Der Grundsatz der Speicherbegrenzung knüpft in zeitlicher Hinsicht an die Grundsätze der Zweckbindung und Datenminimierung an.[32] Personenbezogene Daten sollen nur so lange in einer Form gespeichert werden, die eine Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Damit dürfen Daten nur dann für einen unbegrenzten Zeitraum aufbewahrt werden, wenn sie anonym sind. Das setzt unter den Voraussetzungen von Big Data in der Regel mehr voraus als die Löschung des Namens und weiterer unmittelbar identifizierbarer Merkmale. Ob 136

30 Schantz, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, Art. 5 Rn. 26; Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 3. Auflage 2021, Art. 5 Rn. 35.

31 Schantz, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, Art. 5 Rn. 29; Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 3. Auflage 2021, Art. 5 Rn. 41.

32 Schantz, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, Art. 5 Rn. 32; Böhm/Ströbel, in: Wybitul, EU-Datenschutz-Grundverordnung, Teil II, Art. 5 Rn. 27.

Daten wirksam anonymisiert wurden, lässt sich letztlich nur im konkreten Fall entscheiden.

137 Die DSGVO widmet der Speicherbegrenzung einen eigenständigen Grundsatz. Das macht deutlich, welche Bedeutung sie diesem Aspekt beimisst.[33] In der Praxis ist der Verantwortliche gehalten, den Grundsatz durch Entwicklung und Umsetzung eines Löschkonzepts ins Werk zu setzen. Für die unterschiedlichen verarbeiteten Datenkategorien sollten dabei individuelle Löschfristen festgelegt und in dem Verzeichnis der Verarbeitungstätigkeiten dokumentiert werden.

2.3.8 Integrität und Vertraulichkeit

138 Mit dem Grundsatz der Integrität und Vertraulichkeit führt die DSGVO ein neues Datenschutzprinzip ein. Die Datenschutz-Richtlinie 95/46/EG kannte diesen Grundsatz nicht. Die Prinzipien Integrität und Vertraulichkeit dienen der Verwirklichung der Datensicherheit. Die beschriebenen Prinzipien stellen klassische Schutzziele der Informationssicherheit dar.

139 Kern des Grundsatzes ist die Aufforderung an den Verantwortlichen, personenbezogene Daten in einer Art und Weise zu verarbeiten, die eine angemessene Sicherheit gewährleistet. Dazu trifft der Verantwortliche technische und organisatorische Maßnahmen, die geeignet sind, eine unbefugte oder unrechtmäßige Verarbeitung, einen unbeabsichtigten Verlust, eine unbeabsichtigte Zerstörung oder unbeabsichtigte Schädigung zu verhindern. Art. 32 Abs. 1 DSGVO konkretisiert diese Vorgaben. Art und Umfang der zu treffenden Maßnahmen hängt dabei insbesondere von der Sensibilität der verarbeiteten Daten, der Datenmenge und den Risiken für die Rechte und Freiheiten der betroffenen Personen im Fall eines unbefugten Zugriffs auf die Daten ab.

140 Integrität beschreibt die Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.[34] Daten sollen nicht gelöscht, vernichtet oder unbefugt verändert werden. Vertraulichkeit zielt auf den Schutz der Daten vor unbefugter Kenntnisnahme und damit vor unbefugter Verarbeitung. Daten dürfen ausschließlich Befugten zugänglich sein.[35]

141 Anders als die in § 9 BDSG-alt und seiner Anlage konkret benannten acht Kontrollziele (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle etc.), eröffnet der Grundsatz der Integrität und Vertraulichkeit zusammen mit seiner Konkretisierung in Art. 32 Abs. 1 DSGVO dem Verantwortlichen einen größeren Spielraum bei der Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen. Entscheidend ist allein, dass die getroffenen Maßnahmen mit

33 Schantz, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, DS-GVO, Art. 5 Rn. 32.

34 Online-Glossar des Bundesamtes für Sicherheit in der Informationstechnik, *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html* (letzter Abruf: 09. 11. 2020).

35 Online-Glossar des Bundesamtes für Sicherheit in der Informationstechnik, *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html* (letzter Abruf: 09. 11. 2020).

Blick auf die bei der Verarbeitung durch den Verantwortlichen identifizierten Risiken ein angemessenes Schutzniveau bieten.

2.3.9 Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO weist dem Verantwortlichen – sprachlich redundant, rechtlich aber konstitutiv – die Verantwortlichkeit für die Einhaltung der zuvor näher beschriebenen Datenschutzgrundsätze zu. Dieser Grundsatz war bereits in der Datenschutz-Richtlinie 95/46/EG enthalten (siehe Art. 6 Abs. 2) und regelt insofern Altbekanntes. Die Regelung macht deutlich, dass es sich bei den Datenschutzgrundsätzen des Art. 5 Abs. 1 DSGVO nicht bloß um Programmsätze handelt, deren Nichteinhaltung für den Verantwortlichen folgenlos bleibt. Die Datenschutzgrundsätze enthalten vielmehr konkrete Handlungsaufträge für den Verantwortlichen, die mit Blick auf die von diesem durchgeführten Verarbeitungstätigkeiten angewandt werden müssen. 142

Neben dieser Verpflichtung führt die DSGVO ein neues Element ein. Sie verpflichtet den Verantwortlichen, die Einhaltung der Datenschutzgrundsätze jederzeit nachweisen zu können. Diese beiden Aspekte fasst die DSGVO unter dem Begriff der Rechenschaftspflicht („Accountability") zusammen. 143

Den Grundsatz der Rechenschaftspflicht konkretisieren die Regelungen des Art. 24 Abs. 1 DSGVO. Danach obliegt es dem Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den Vorschriften der DSGVO erfolgt. Die von dem Verantwortlichen getroffenen Maßnahmen sollen regelmäßig überprüft und aktualisiert werden. 144

Das erfordert die Etablierung eines Datenschutz-Managementsystems im Unternehmen, um die gesetzlichen Anforderungen des Datenschutzes systematisch planen, organisieren, steuern und kontrollieren zu können. Aufgrund der Nachweispflicht müssen die eingerichteten Datenschutzprozesse dokumentiert und ihre Wirksamkeit regelmäßig überprüft werden.[36] Verstöße gegen die Bestimmungen der DSGVO können so frühzeitig erkannt und durch Ergreifen geeigneter Maßnahmen beseitigt werden. Auf diese Weise wird das Datenschutz-Management zu einem wesentlichen Element des im Unternehmen eingerichteten Compliance-Managementsystems.[37] 145

Die Einführung der Nachweispflicht kehrt die Beweislast in Kontrollverfahren der Aufsichtsbehörde zuungunsten des Verantwortlichen um.[38] Für Unterneh- 146

36 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil II, 1. Auflage 2017 Datenschutzorganisation Kapitel 1. Datenschutzmanagement und Datenschutzprozesse, Rn. 2.

37 Schantz, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 05. 2020, Art. 5 Rn. 38.

38 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil II. Datenschutzorganisation Kapitel 1. Datenschutzmanagement und Datenschutzprozesse, Rn. 4; Böhm/Ströbel, in: Wybitul, EU-Datenschutz-Grundverordnung, Teil II, 1. Auflage 2017, Art. 5 Rn. 42.

men ist es daher von besonderer Bedeutung, sämtliche Maßnahmen zu dokumentieren, die es zur Einhaltung der gesetzlichen Datenschutzvorschriften getroffen hat.

147 Um den Grundsatz der Rechenschaftspflicht zu erfüllen, sollte ein Unternehmen in Anlehnung an die Vorgaben der Artikel 29-Datenschutzgruppe die Umsetzung dieser Maßnahmen in Betracht ziehen:[39]

- Benennung eines Datenschutzbeauftragten;
- frühzeitige Einbindung des Datenschutzbeauftragten bei Einführung neuer Verarbeitungen;
- Festlegung von verbindlichen Datenschutzrichtlinien;
- Führung des Verzeichnisses von Verarbeitungstätigkeiten;
- Durchführung von Schulungen zum Datenschutz;
- Festlegung eines Verfahrens für die Wahrnehmung der Betroffenenrechte;
- Einrichtung einer Stelle für die Bearbeitung von Beschwerden;
- Festlegung eines Verfahrens für den Umgang mit Datenschutzverletzungen;
- Durchführung von internen und externen Audits zur Überwachung der bestehenden Datenschutzrichtlinien.

2.4 Betroffenenrechte

148 Kapitel III der DSGVO enthält die Rechte der betroffenen Person. Die betroffene Person hat das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Diese Rechte versetzen die betroffene Person in die Lage, ihre Interessen mit Blick auf den Umgang mit ihren personenbezogenen Daten gegenüber dem Verantwortlichen (nicht: dem Auftragsverarbeiter) geltend zu machen und durchzusetzen. Die individuellen Datenschutzrechte zu stärken, war ein wichtiges Anliegen der europäischen Datenschutzreform.[40]

149 Die Ausübung dieser Rechte ist gem. Art. 12 Abs. 5 S. 1 DSGVO grundsätzlich **kostenfrei.** Macht die betroffene Person von ihrem Recht Gebrauch, hat der Verantwortliche die begehrte Maßnahme im Regelfall **binnen eines Monats** durchzuführen. Verstöße können die Aufsichtsbehörden gem. Art. 83 Abs. 5 lit. b DSGVO mit einem Bußgeld ahnden.

2.4.1 Auskunft

150 Das Recht auf Auskunft ist **das zentrale Datenschutzrecht** der betroffenen Person.[41] Es versetzt die betroffene Person in die Lage zu erfahren, welche personenbezogenen Daten zu ihr bei dem Verantwortlichen gespeichert sind.

39 Artikel 29-Datenschutzgruppe, WP 173 vom 13. 07. 2010, S. 12 f.
40 Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. Auflage 2016, S. 83.
41 Dix, in: Simits, Bundesdatenschutzgesetz, 8. Auflage 2014, § 34 Rn. 1.

Nur wenn diese Kenntnis gegeben ist, können auch Folgerechte, wie z. B. Berichtigung und Löschung, sinnvoll ausgeübt werden.

Das Auskunftsrecht ist in Art. 15 DSGVO verankert. Sein Umfang ergibt sich aus Art. 15 Abs. 1 und 2 DSGVO. Danach hat die betroffene Person Anspruch auf Mitteilung dieser Informationen: 151

- personenbezogene Daten, die der Verantwortliche zu der betroffenen Person verarbeitet;
- Verarbeitungszwecke;
- Kategorien der verarbeiteten personenbezogenen Daten;
- Empfänger oder Kategorien von Empfängern der verarbeiteten personenbezogenen Daten;
- Speicherdauer oder Kriterien für die Festlegung der Speicherdauer;
- Hinweis auf die Datenschutzrechte der betroffenen Person;
- Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde;
- Informationen über die Herkunft der Daten;
- Informationen über eine automatisierte Entscheidungsfindung einschließlich Profiling;
- Information über die geeigneten Garantien gem. Art. 46 DSGVO bei Datenübermittlung an ein Drittland oder eine internationale Organisation.

Das Auskunftsrecht ist **zweistufig** ausgestaltet. Zunächst hat die betroffene Person das Recht auf Mitteilung, ob der Verantwortliche sie betreffende personenbezogene Daten speichert (Stufe 1). Wenn der Verantwortliche dies bestätigt, kann Auskunft über die gespeicherten personenbezogenen Daten verlangt werden (Stufe 2). 152

In der Praxis werden die Stufen 1 und 2 häufig zusammenfallen. Die betroffene Person wird in der Regel sogleich um Mitteilung bitten, welche sie betreffenden Daten bei dem Verantwortlichen gespeichert sind. Stellt der Verantwortliche bei der Prüfung dieses Antrags fest, dass zu der betroffenen Person keine Daten vorhanden sind, verfährt er gem. Art. 12 Abs. 4 DSGVO. Dies umfasst die Mitteilung an die betroffene Person, dass keine sie betreffenden Daten gespeichert sind (Negativauskunft). 153

Gem. Art. 15 Abs. 3 S. 1 DSGVO ist der Verantwortliche verpflichtet, der betroffenen Person eine **Kopie** ihrer personenbezogenen Daten als Bestandteil der Auskunft bereitzustellen. Gemeint ist hiermit eine grafische Nachbildung der bei dem Verantwortlichen gespeicherten Daten, und zwar so, wie sie bei dem Verantwortlichen wahrnehmbar sind.[42] Die Bereitstellung der Datenkopie muss in einem gängigen elektronischen Format erfolgen (Art. 15 Abs. 3 S. 3 DSGVO), wie z. B. PDF oder CSV.[43] 154

42 Engeler/Quiel, NJW 2019, 2201, 2203.

43 Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Auflage 2016, S. 142 f.

2.4.2 Berichtigung

155 Die betroffene Person kann von dem Verantwortlichen verlangen, dass sie betreffende unrichtige personenbezogene Daten berichtigt werden. Dieses Recht ist in Art. 16 S. 1 DSGVO enthalten und konkretisiert den in Art. 5 Abs. 1 lit. d DSGVO formulierten Grundsatz der Richtigkeit von Daten. Der Anspruch aus Art. 16 DSGVO ist unabdingbare Voraussetzung für dessen wirksame Durchsetzung gegenüber dem Verantwortlichen.

156 Je nach Umfang, Art und Zweck der Verarbeitung kann der Berichtigungsanspruch für die betroffene Person unterschiedliche Bedeutung haben. Sind in dem Profil einer Person, welches für die Ausspielung von personalisierter Werbung verwendet wird, deren Interessen falsch erfasst oder ermittelt worden, sind die Beeinträchtigungen für die Rechte und Freiheiten der betroffenen Person zu vernachlässigen. Die Auswirkungen werden eher für den Verantwortlichen negativ sein, erfolgt die Ausspielung der Werbung durch die unzutreffenden Profilangaben doch weniger passgenau. Die zu erwartenden Geschäftsabschlüsse werden daher voraussichtlich weniger erfolgreich sein. Speichert eine Auskunftei hingegen falsche Bonitätsdaten über die betroffene Person, können ihre Rechte und Freiheiten spürbar beeinträchtigt sein, indem z. B. ein Kredit nicht gewährt oder bestehende Kreditlinien widerrufen werden.

157 Um dem Berichtigungsanspruch in einer Zeit, in der Daten in Bruchteilen von Sekunden an Dritte übermittelt werden können, eine möglichst umfassende Geltung zu verschaffen, verpflichtet Art. 19 S. 1 DSGVO den Verantwortlichen, sämtliche Empfänger, denen die personenbezogenen Daten der betroffenen Person mitgeteilt wurden, über eine vorgenommene Berichtigung zu unterrichten. Diese Unterrichtungspflicht gilt ausnahmsweise nicht, wenn die Unterrichtung der Empfänger dem Verantwortlichen unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist.

158 Neben dem Berichtigungsanspruch enthält Art. 16 S. 2 DSGVO das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Dabei werden richtig gespeicherte personenbezogene Daten um zusätzliche Angaben ergänzt, die das ursprüngliche Datum erläutern oder dessen Bedeutungsgehalt verändern.[44] Die Vervollständigung kann auch mithilfe einer ergänzenden Erklärung vorgenommen werden. Für das Bestehen des Anspruchs und seine Reichweite sind die Zwecke der von dem Verantwortlichen durchgeführten Verarbeitung maßgeblich.

2.4.3 Löschung

159 Art. 17 DSGVO regelt das Recht auf Löschung. Im Untertitel bezeichnet die DSGVO dieses Recht auch als Recht auf Vergessenwerden. Ein qualitatives Mehr gegenüber dem herkömmlichen Recht auf Löschung ist damit jedoch nicht verbunden.

44 Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Auflage 2016, S. 146.

Der Verantwortliche ist verpflichtet, personenbezogene Daten auf Verlangen der betroffenen Person zu löschen, wenn einer der folgenden Tatbestände gegeben ist: 160

- Erreichung/Erfüllung des Verarbeitungszwecks;
- Widerruf der Einwilligung und kein anderweitiger Erlaubnistatbestand für die Verarbeitung gegeben;
- Widerspruch gegen die Verarbeitung und keine vorrangigen berechtigten Gründe für die Verarbeitung gegeben;
- Widerspruch gegen die Verarbeitung für Zwecke der Direktwerbung;
- unrechtmäßige Verarbeitung;
- Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten;
- Verarbeitung von personenbezogenen Daten eines Kindes bei einem Online-Dienst.

Den Begriff „Löschen" definiert die DSGVO nicht. Gemäß § 3 Abs. 4 Nr. 5 BDSG-alt bedeutete Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten. Das Unkenntlichmachen ist jede Handlung, die dazu führt, dass Daten nicht mehr zur Kenntnis genommen und Informationen nicht länger aus gespeicherten Daten gewonnen werden können.[45] Die Handlung darf nicht reversibel sein. 161

Hat der Verantwortliche die personenbezogenen Daten der betroffenen Person öffentlich gemacht, verpflichtet Art. 17 Abs. 2 DSGVO diesen, Dritte, die die Daten verarbeiten, über das Löschverlangen zu informieren. Dieses Recht auf Vergessenwerden ist beschränkt. Bei der Umsetzung darf der Verantwortliche die verfügbare Technologie und die Implementierungskosten der von ihm in Aussicht genommenen Maßnahmen berücksichtigen. 162

Ergänzend zu dem Recht auf Vergessenwerden verpflichtet Art. 19 DSGVO den Verantwortlichen, alle Empfänger, denen personenbezogenen Daten übermittelt wurden, über eine Löschung von personenbezogenen Daten zu informieren. Diese Informationspflicht trifft den Verantwortlichen nicht, wenn die Benachrichtigung der Empfänger unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. 163

Das Recht auf Löschung besteht nicht unbeschränkt. Der Verantwortliche ist gem. Art. 17 Abs. 3 DSGVO nicht verpflichtet, personenbezogene Daten auf Verlangen der betroffenen Person zu löschen, wenn die weitere Verarbeitung aufgrund einer der folgenden Tatbestände erforderlich ist: 164

- Ausübung des Rechts auf freie Meinungsäußerung und Information;
- Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder Wahrnehmung einer dem Verantwortlichen

45 Schild, in: BeckOK Datenschutzrecht Wolff/Brink (Hrsg.), Stand: 01. 08. 2017, § 3 Rn. 86.

übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt;
- Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke;
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

165 Bei nicht automatisierter Datenverarbeitung besteht gem. § 35 Abs. 1 BDSG-neu ebenfalls kein Recht auf Löschung, wenn wegen der besonderen Art der Speicherung eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.

166 Für Unternehmen werden die Tatbestände „Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten" sowie „Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen" die größte Bedeutung für die Befreiung von der Löschpflicht erlangen. Typisches Beispiel ist das Bestehen von handels- oder steuerrechtlichen Aufbewahrungspflichten gem. § 147 AO und § 257 HGB.

167 In der Gesamtschau ist das Recht auf Löschung in der DSGVO etwas stärker ausgestaltet als im BDSG-alt. Grund hierfür ist, dass aus dem BDSG-alt bekannte Ausnahmen vom Recht auf Löschung keinen Eingang in die DSGVO gefunden haben. So entfällt für den Bereich der automatisierten Datenverarbeitung die Möglichkeit des § 35 Abs. 3 Nr. 3 BDSG-alt, personenbezogene Daten zu sperren, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

2.4.4 Einschränkung der Verarbeitung

168 Gemäß Art. 18 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen. In § 35 Abs. 3, 4 BDSG-alt war die Einschränkung der Verarbeitung unter dem Begriff „Sperrung" bekannt. Art. 4 Nr. 3 DSGVO definiert den Begriff „Einschränkung der Verarbeitung" als die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

169 Der Verantwortliche ist verpflichtet, die Verarbeitung personenbezogener Daten der betroffenen Person auf Verlangen einzuschränken, wenn einer der folgenden Tatbestände gegeben ist:
- Bestreiten der Richtigkeit personenbezogener Daten von der betroffenen Person für den Prüfzeitraum des Verantwortlichen;
- Verarbeitung unrechtmäßig und Ablehnung der Löschung der personenbezogenen Daten durch die betroffene Person;

– Verwendung für Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen durch die betroffene Person, obwohl Erreichung/Erfüllung des Verarbeitungszwecks;
– Widerspruch gegen Verarbeitung für den Prüfzeitraum des Verantwortlichen.

Sind die Voraussetzungen für die Einschränkung der Verarbeitung gegeben, darf der Verantwortliche die Daten gem. Art. 18 Abs. 2 DSGVO nur noch speichern. Darüber hinaus darf keine Verarbeitung der Daten erfolgen. Dieses strenge Verarbeitungsverbot gilt nicht, wenn die betroffene Person in die weitere Verarbeitung einwilligt, die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats erforderlich ist. 170

2.4.5 Datenübertragbarkeit

Mit dem Recht auf Datenübertragbarkeit führt die DSGVO ein neues Recht für die betroffene Person ein. Das Recht bildet im Datenschutzrecht einen Fremdkörper. Es verfolgt mit dem Ziel, Monopolstrukturen zu verhindern und den Wechsel von Anbietern zu erleichtern, einen anderen Schutzzweck als den Schutz des Rechts auf informationelle Selbstbestimmung.[46] In der Stellungnahme der Artikel 29-Datenschutzgruppe vom 13. 12. 2016 heißt es hierzu:[47] 171

> *„Indeed, the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). It also enables the creation of new services in the context of the digital single market strategy."*

Gleichwohl hat das Recht auf Datenübertragbarkeit in Art. 20 DSGVO Eingang in die datenschutzrechtlichen Vorschriften gefunden. Unternehmen müssen sich mit dem Recht daher befassen und die Voraussetzungen für seine Umsetzung schaffen. 172

Das Recht auf Datenübertragbarkeit findet nur Anwendung, wenn die Verarbeitung auf einer **Einwilligung** oder auf einem **Vertrag** beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Verarbeitet der Verantwortliche personenbezogene Daten aufgrund eines überwiegenden berechtigten Interesses, greift das Recht auf Datenübertragbarkeit nicht. Ebenso kommt ein Recht auf Datenübertragbarkeit nicht in Betracht, wenn der Verantwortliche die Daten lediglich in Papierform verarbeitet. 173

Sind die genannten Voraussetzungen gegeben, kann die betroffene Person gem. Art. 20 Abs. 1 DSGVO von dem Verantwortlichen verlangen, die sie betreffenden personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt hat, in einem **strukturierten, gängigen und maschinenlesbaren Format** zu erhalten. 174

46 Hornung, ZD 2012, 99, 103.
47 Artikel 29-Datenschutzgruppe, WP 242 vom 13. 12. 2014, S. 4.