

The top half of the cover features a dark background with a pattern of binary code (0s and 1s) in light blue and green. Overlaid on this is a large, stylized graphic of a padlock, rendered in a grid of white and yellow squares. The padlock is positioned in the upper right quadrant. To the left of the padlock, there are several concentric, glowing circles in shades of orange and yellow, creating a sense of depth and focus.

Paul Voigt
Axel von dem Bussche

Inklusive
BDSG-neu

EU-Datenschutz- Grundverordnung (DSGVO)

Praktikerhandbuch

 Springer

EU-Datenschutz-Grundverordnung (DSGVO)

Paul Voigt
Axel von dem Bussche

EU-Datenschutz- Grundverordnung (DSGVO)

Praktikerhandbuch

unter vollständiger Berücksichtigung des deutschen
Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU
(DSAnpUG-EU)



Springer

Paul Voigt
Taylor Wessing
Berlin
Deutschland

Axel von dem Bussche
Taylor Wessing
Hamburg
Deutschland

ISBN 978-3-662-56186-7 ISBN 978-3-662-56187-4 (eBook)
<https://doi.org/10.1007/978-3-662-56187-4>

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

© Springer-Verlag GmbH Germany 2018

Erweiterte Übersetzung der englischen Ausgabe: The EU General Data Protection Regulation (GDPR) von Paul Voigt und Axel von dem Bussche, © Springer International Publishing AG 2017. Alle Rechte vorbehalten.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil von Springer Nature

Die eingetragene Gesellschaft ist Springer-Verlag GmbH Deutschland

Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Personenbezogene Daten spielen für Unternehmen eine zunehmend wichtige Rolle. Sie sind längst ein bedeutendes Wirtschaftsgut und werden alltäglich zur Durchführung von internen wie externen Geschäftsprozessen erhoben und verarbeitet. Zum Schutz der Rechte und Freiheiten der betroffenen Personen findet aus diesem Grunde gleichlaufend eine Verschärfung von Datenschutzpflichten statt, deren Umsetzung Unternehmen vor eine komplexe Aufgabe stellt. Diese agieren heute regelmäßig grenzüberschreitend und auch Datenflüsse machen vor Landesgrenzen keinen Halt. Bisher sahen sich Unternehmen daher mit der Herausforderung konfrontiert, mehrere nationale Datenschutzregime gleichzeitig berücksichtigen zu müssen. Dies hemmte den grenzüberschreitenden Datenaustausch. Eine diesbezügliche Abhilfe in Europa soll ab Mai 2018 die EU-Datenschutz-Grundverordnung („DSGVO“) schaffen. Diese harmonisiert das Datenschutzrecht in allen EU-Mitgliedstaaten und findet aufgrund ihres weiten Anwendungsbereichs nicht nur auf in der EU ansässige Unternehmen Anwendung, sondern stellt zugleich ein Pflichtenprogramm für solche Unternehmen auf, die auf dem Binnenmarkt tätig sind. Bei einer Verletzung der datenschutzrechtlichen Pflichten drohen Bußgelder in Millionenhöhe.

Dieses Handbuch soll Unternehmen – auch solchen mit Konzernstrukturen – praxisorientierte, verständliche und fundierte Hinweise und Hilfestellungen zur Umsetzung der DSGVO geben. Dabei werden die datenschutzrechtlichen Grundlagen nicht nur erläutert, sondern zugleich mit Praxisbeispielen illustriert. Die sich in Deutschland auf Grundlage des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU („BDSG-neu“) ergebenden Besonderheiten wurden dabei umfassend berücksichtigt und dargestellt. Dem Handbuch ist außerdem eine „Checkliste“ der wichtigsten Datenschutzpflichten vorangestellt, die maßgebliche Problemfelder in Kurzform darlegt und Verweise auf die entsprechenden Teile dieses Buches enthält. Ein Annex enthält die Normen der DSGVO und verknüpft diese mit den relevanten Erwägungsgründen sowie den zugehörigen Normen des BDSG-neu, sodass alle maßgeblichen Normen übersichtlich abgebildet werden. Gleichzeitig verweist der Annex in die zugehörigen Kapitel des Handbuchs – das Handbuch kann also auch ähnlich wie ein Kommentar verwendet werden, da der Annex die Recherche anhand konkreter Artikel der DSGVO gestattet.

Bei der Entstehung dieses Handbuches konnten wir auf langjährige Praxiserfahrung bei der umfassenden Beratung deutscher, europäischer sowie außereuropäischer

Unternehmen in datenschutzrechtlichen Fragestellungen zurückgreifen. Dabei lassen wir den Leser an unserem Praxiswissen im europäischen wie deutschen Datenschutzrecht teilhaben.

Ausgehend von der hohen Praxisrelevanz der künftigen Rechtsänderungen durch die DSGVO ist zudem unser englischsprachiges Praxishandbuch „EU General Data Protection Regulation – A practical guide“, das „Schwesterwerk“ zu diesem Handbuch jüngst in Erstauflage bei Springer Nature erschienen. Beide Handbücher ermöglichen zusammen eine umfassende Erfassung des künftigen Datenschutzrechts aus europäischer und nationaler Perspektive in deutscher sowie englischer Sprache. Besonders für in internationalen Konzernen tätige deutsche Juristen bietet die gebündelte Verwendung beider Werke die Möglichkeit, nationale Besonderheiten in einen globalen Kontext zu setzen und Kollegen außerhalb Deutschlands verständlich zu machen.

Für die umfassende Unterstützung bei beiden Projekten möchten wir uns bei Frau Dr. Brigitte Reschke und Frau Julia Bieler vom Verlag Springer Nature, sowie unserer herausragenden wissenschaftlichen Mitarbeiterin Rita Danz bedanken.

Stets dankbar sind wir auch für Hinweise, Anregungen und Kritik zu diesem Buch, die Sie gerne per Email an p.voigt@taylorwessing.com oder a.bussche@taylorwessing.com richten können.

Berlin und Hamburg, August 2017

Paul Voigt
Axel Freiherr von dem Bussche

Inhaltsverzeichnis

1	Einleitung und „Checkliste“	1
1.1	Gesetzgeberischer Hintergrund und bisherige Rechtslage	1
1.1.1	Die EG-Datenschutzrichtlinie	1
1.1.2	Die Datenschutz-Grundverordnung	2
1.1.3	Das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU	3
1.2	Checkliste – Die wichtigsten datenschutzrechtlichen Pflichten	4
1.2.1	Datenschutzorganisation	4
1.2.2	Rechtmäßigkeit der Datenverarbeitung	7
	Referenzen	9
2	Anwendungsbereich der DSGVO	11
2.1	In welchen Fällen ist die Verordnung anwendbar? – sachlicher Anwendungsbereich	11
2.1.1	„Verarbeitung“	11
2.1.2	„Personenbezogene Daten“	13
2.1.3	Ausnahmen vom sachlichen Anwendungsbereich	19
2.2	Auf wen ist die Verordnung anwendbar? – persönlicher Anwendungsbereich	20
2.2.1	„Verantwortlicher“	21
2.2.2	„Auftragsverarbeiter“	24
2.2.3	Von der DSGVO geschützte Personen	25
2.3	Wo ist die Verordnung anwendbar? – räumlicher Anwendungsbereich	25
2.3.1	Datenverarbeitung im Rahmen der Tätigkeiten einer EU-Niederlassung	27
2.3.2	Verarbeitung personenbezogener Daten von innerhalb der EU befindlichen betroffenen Personen	31
2.4	Anwendungsbereich des BDSG-neu	34
	Referenzen	36
3	Anforderungen an die Datenschutzorganisation	39
3.1	Rechenschaftspflicht	39
3.2	Allgemeine Pflichten	41

3.2.1	Verantwortlichkeit, Haftung und allgemeine Pflichten des Verantwortlichen	41
3.2.2	Die Verteilung von Verantwortlichkeiten zwischen gemeinsam für die Verarbeitung Verantwortlichen („Joint controllers“)	43
3.2.3	Zusammenarbeit mit den Aufsichtsbehörden	46
3.3	Technische und organisatorische Maßnahmen	47
3.3.1	Angemessenes Datenschutzniveau	48
3.3.2	Mindestanforderungen	48
3.3.3	Risikobasierter Ansatz bezüglich Datenschutz	50
3.3.4	Die NIS-Richtlinie	52
3.4	Verzeichnisse über Verarbeitungstätigkeiten	54
3.4.1	Inhalt und Zweck der Verzeichnisse	54
3.4.2	Dokumentation der Zwecke der Datenverarbeitung	55
3.4.3	Ausnahme von der Pflicht zum Führen der Verzeichnisse	56
3.5	Datenschutz-Folgenabschätzung („Data Protection Impact Assessment“)	58
3.5.1	Betroffene Arten von Verarbeitungstätigkeiten	59
3.5.2	Vornahme der Folgenabschätzung	60
3.6	Datenschutzbeauftragter	65
3.6.1	Pflicht zur Benennung	66
3.6.2	Anforderungen an den Datenschutzbeauftragten	72
3.6.3	Stellung des Datenschutzbeauftragten	75
3.6.4	Aufgaben des Datenschutzbeauftragten	78
3.7	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy by Design and by Default“)	81
3.8	Verletzungen des Schutzes personenbezogener Daten („Data Breach Notification“)	84
3.8.1	Verletzung des Schutzes personenbezogener Daten	84
3.8.2	Meldung an die Aufsichtsbehörde	85
3.8.3	Benachrichtigung der betroffenen Personen	89
3.9	Verhaltensregeln, Zertifizierungen, Siegel, etc.	92
3.9.1	Verhältnis zwischen Verhaltensregeln und Zertifizierungen	92
3.9.2	Verhaltensregeln („Codes of Conduct“)	94
3.9.3	Zertifizierungen, Datenschutzsiegel und –prüfzeichen („Certifications, seals and marks“)	99
3.10	Auftragsverarbeiter	103
3.10.1	Privilegierte Stellung des Auftragsverarbeiters	103
3.10.2	Verpflichtung des Verantwortlichen bei der Auswahl eines Auftragsverarbeiters	104
3.10.3	Pflichten des Auftragsverarbeiters	106
3.10.4	Hinzuziehung eines „Unter-Auftragsverarbeiters“	108
	Referenzen	108

4	Materielle Anforderungen	113
4.1	Verarbeitungsgrundsätze	113
4.1.1	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	114
4.1.2	Zweckbindung	115
4.1.3	Datenminimierung	117
4.1.4	Richtigkeit	118
4.1.5	Speicherbegrenzung	118
4.1.6	Integrität und Vertraulichkeit	119
4.2	Rechtsgrundlagen für die Datenverarbeitung	119
4.2.1	Verarbeitung auf der Grundlage der Einwilligung der betroffenen Person	119
4.2.2	Verarbeitung auf der Grundlage eines gesetzlichen Erlaubnistatbestandes	129
4.2.3	Verarbeitung besonderer Kategorien personenbezogener Daten	145
4.3	Datenübermittlungen an Drittländer	155
4.3.1	Angemessenheitsbeschlüsse	157
4.3.2	Einwilligung	158
4.3.3	Standardvertragsklauseln	159
4.3.4	EU-U.S. Privacy Shield	163
4.3.5	Binding Corporate Rules	166
4.3.6	Verhaltensregeln, Zertifizierungsverfahren, etc.	171
4.3.7	Ausnahmen für bestimmte Fälle	172
4.3.8	Benennung eines Vertreters durch nicht in der EU niedergelassene Unternehmen	176
4.4	Eingeschränktes „Konzernprivileg“	178
4.4.1	Eigenständige Datenschutzverantwortlichkeit jedes Gruppenunternehmens	179
4.4.2	Erleichterungen in Bezug auf die materiellen Anforderungen	180
4.4.3	Erleichterungen in Bezug auf die Datenschutzorganisation	181
	Referenzen	182
5	Rechte der betroffenen Personen	185
5.1	Transparenz und Modalitäten	185
5.1.1	Die Art und Weise der Kommunikation mit den betroffenen Personen	186
5.1.2	Die Form der Kommunikation	187
5.2	Informationspflicht des Verantwortlichen bei Erhebung der personenbezogenen Daten	188
5.2.1	Zeitpunkt der Information	189

5.2.2	Erhebung der Daten bei der betroffenen Person	189
5.2.3	Erhebung der Daten von einer anderen Quelle	191
5.2.4	Einschränkung der Informationspflichten nach dem BDSG-neu	192
5.2.5	Praxishinweise	195
5.3	Informationen über auf den Antrag der betroffenen Personen hin ergriffene Maßnahmen.	196
5.3.1	Art und Weise der Bereitstellung der Informationen.	196
5.3.2	Frist für die Bereitstellung der Informationen.	198
5.3.3	Unterrichtung im Falle Nicht-Tätigwerdens	198
5.3.4	Bestätigung der Identität der betroffenen Person.	199
5.4	Auskunftsrecht	199
5.4.1	Umfang des Auskunftsrechts	199
5.4.2	Einschränkungen des Auskunftsrechts nach dem BDSG-neu	201
5.4.3	Zurverfügungstellen der personenbezogenen Daten	203
5.4.4	Praxishinweise	205
5.5	Recht auf Löschung, auf Berichtigung und auf Einschränkung der Verarbeitung.	206
5.5.1	Recht auf Berichtigung	206
5.5.2	Recht auf Löschung	208
5.5.3	Recht auf Einschränkung der Verarbeitung	220
5.5.4	Mitteilungspflicht gegenüber Dritten im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung, Art. 19 . .	224
5.6	Recht auf Datenübertragbarkeit	225
5.6.1	Anwendungsbereich & Ausübung des Rechts auf Datenübertragbarkeit	226
5.6.2	Technische Spezifikationen	232
5.6.3	Übermittlung der Daten	233
5.6.4	Verhältnis zum Recht auf Löschung	233
5.6.5	Ausschluss des Rechts auf Datenübertragbarkeit	234
5.7	Widerspruchsrecht	235
5.7.1	Gründe für einen Widerspruch gegen die Verarbeitung. . . .	236
5.7.2	Einschränkungen im BDSG-neu	238
5.7.3	Ausübung des Rechts & Rechtsfolgen.	239
5.7.4	Informationspflicht.	240
5.8	Automatisierte Entscheidungsfindung	240
5.8.1	Anwendungsbereich des Verbots	241
5.8.2	Ausnahmen vom Verbot nach der DSGVO	243
5.8.3	Ausnahme vom Verbot nach dem BDSG-neu	244
5.8.4	Angemessene Schutzmaßnahmen	245
5.9	Beschränkungen der Betroffenenrechte	246
	Referenzen	247

6	Zusammenarbeit mit den Aufsichtsbehörden	251
6.1	Bestimmung der zuständigen Aufsichtsbehörde	251
6.2	One-Stop-Shop	252
6.3	Bestimmung der federführenden Aufsichtsbehörde	254
6.3.1	Bestimmung anhand der Hauptniederlassung des Unternehmens	254
6.3.2	Bestimmung bei Fehlen einer Niederlassung des Unternehmens in der EU	257
6.3.3	Ausnahme: lokale Zuständigkeit	258
6.3.4	One-Stop-Shop auf nationaler Ebene nach dem BDSG-neu	259
6.4	Zusammenarbeit und Kohärenzverfahren	260
6.4.1	Europäischer Datenschutzausschuss	261
6.4.2	Verfahren zur Zusammenarbeit	261
6.4.3	Kohärenzverfahren	262
	Referenzen	262
7	Rechtsdurchsetzung und Sanktionen nach der DSGVO	265
7.1	Aufgaben und Untersuchungsbefugnisse der Aufsichtsbehörden	265
7.1.1	Größere Konsistenz der Untersuchungsbefugnisse innerhalb der EU	266
7.1.2	Regelungen zu aufsichtsbehördlichen Befugnissen im BDSG-neu	266
7.1.3	Umfang der Untersuchungsbefugnisse	268
7.1.4	Ausübung der Befugnisse	270
7.2	Zivilrechtliche Haftung	270
7.2.1	Recht auf Schadensersatz	271
7.2.2	Schadensersatzpflichtige	273
7.2.3	Exkulpationsmöglichkeit	274
7.3	Sanktionen	275
7.3.1	Abhilfebefugnisse der Aufsichtsbehörden	276
7.3.2	Gründe für Bußgelder und Bußgeldbeträge	277
7.3.3	Verhängung von Bußgeldern, inkl. mildernden Umständen	278
7.3.4	Sanktionierung von Unternehmensgruppen	279
7.3.5	Sanktionen und Verfahrensvorschriften des BDSG-neu	280
7.3.6	Praxishinweise	282
7.4	Rechtsbehelfe	282
7.4.1	Rechtsbehelfe von datenverarbeitenden Unternehmen	282
7.4.2	Rechtsbehelfe von betroffenen Personen	284
	Referenzen	287
8	Nationale Besonderheiten	289
8.1	Vielzahl von Öffnungsklauseln	289
8.1.1	Öffnungsklauseln innerhalb der allgemeinen Bestimmungen der DSGVO	289

8.1.2	Gesetzgebungskompetenz der EU-Mitgliedstaaten in besonderen Verarbeitungssituationen.	294
8.1.3	Regelungen im BDSG-neu zu besonderen Verarbeitungssituationen.	295
8.2	Beschäftigtendatenschutz.	297
8.2.1	Öffnungsklausel.	297
8.2.2	Regelungen des § 26 BDSG-neu.	299
8.2.3	Arbeitnehmersvertretungsorgan in Deutschland (Betriebsrat).	304
8.3	Telemediendatenschutz.	306
	Referenzen.	309
9	Besondere Verarbeitungssituationen.	311
9.1	Big Data.	311
9.1.1	Anwendbarkeit der DSGVO.	312
9.1.2	Rechenschaftspflicht.	313
9.1.3	Einhaltung der Verarbeitungsgrundsätze.	314
9.2	Cloud Computing.	315
9.2.1	Verteilung der Verantwortlichkeiten.	315
9.2.2	Auswahl eines geeigneten Cloud-Serviceanbieters.	316
9.2.3	Cloud-Serviceanbieter in Drittländern.	317
9.3	Internet of Things.	317
9.3.1	Rechtsgrundlage für Datenverarbeitungen im IoT.	317
9.3.2	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.	319
	Referenzen.	320
10	Praktische Umsetzung der Vorgaben der DSGVO.	321
10.1	Schritt 1: „Lücken“-Analyse.	322
10.2	Schritt 2: Risikoanalyse.	323
10.3	Schritt 3: Projektkonzeption und Ressourcen-/Budgetplanung.	323
10.4	Schritt 4: Implementierung.	324
10.5	Schritt 5: Nationale Zusatzanforderungen.	325
	Referenzen.	326
	Annex I – Gegenüberstellung der Vorschriften und entsprechenden Erwägungsgründe der DSGVO sowie der korrespondierenden Vorschriften des BDSG-neu.	327
	Stichwortverzeichnis.	529

Die rechtlichen Anforderungen an Datenverarbeitungen unterliegen stetem Wandel und für Unternehmen wird es zunehmend schwieriger festzustellen, ob ihre Datenverarbeitungstätigkeiten gesetzeskonform sind. Dies gilt vor allem im internationalen Kontext. Daten können naturgemäß ohne weiteres Landesgrenzen überwinden und spielen in der globalen digitalen Wirtschaft eine zentrale Rolle. In den vergangenen Jahren haben sie sich zu einem wertvollen Wirtschaftsgut entwickelt und werden bereits als „Währung der Zukunft“ bezeichnet.¹ Die Verarbeitung personenbezogener Daten findet im Rahmen zahlloser wirtschaftlicher und sozialer Tätigkeiten statt, wobei Fortschritte in der Informationstechnik die Verarbeitung und den Austausch dieser Daten immer mehr erleichtern.² In diesem Zusammenhang hat der europäische Gesetzgeber die Datenschutz-Grundverordnung (DSGVO) verabschiedet, um eine weitergehende Harmonisierung der Datenschutzregeln innerhalb der EU-Mitgliedstaaten zu erreichen und das Datenschutzniveau zugunsten der von der Verarbeitung betroffenen Personen zu erhöhen. Die DSGVO tritt zum 25. Mai 2018 in Kraft. Aufgrund ihres äußerst weiten, transnationalen Anwendungsbereichs wird sie auch auf zahllose Unternehmen außerhalb der EU Anwendung finden.

1.1 Gesetzgeberischer Hintergrund und bisherige Rechtslage

1.1.1 Die EG-Datenschutzrichtlinie

Vor mehr als 20 Jahren erkannte die Europäische Gemeinschaft (jetzt: Europäische Union) die Notwendigkeit zur Angleichung der Datenschutzstandards in ihren Mitgliedstaaten, um grenzüberschreitende Datenübertragungen innerhalb der EG

¹Reiners, ZD 2015, 51, 55; Martini, in: Paal/Pauly, DSGVO, Art. 25 (2017), Rn. 45 – der Daten als „Rohstoff des 21. Jahrhunderts“ bezeichnet

²ErwGr. 4 EG-Datenschutzrichtlinie

(jetzt: EU) zu erleichtern. Zu dieser Zeit wichen die nationalen Bestimmungen zum Datenschutz stark voneinander ab und konnten keine Rechtssicherheit in Bezug auf grenzüberschreitende Verarbeitungsvorgänge bieten – weder für betroffene Personen, noch für Verantwortliche oder Auftragsverarbeiter.³

1995 verabschiedete die Europäische Gemeinschaft daher die *Richtlinie 95/46/EG* des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (kurz: die *EG-Datenschutzrichtlinie*). Zielstellung war es, den Schutz für die Grundrechte und -freiheiten betroffener Personen im Hinblick auf Datenverarbeitungsvorgänge europaweit zu harmonisieren und den freien Datenverkehr zwischen den EU-Mitgliedstaaten zu gewährleisten.⁴

Richtlinien der Europäischen Union sind in den Mitgliedstaaten nicht direkt anwendbar, sondern bedürfen einer Umsetzung in nationales Recht. Zu diesem Zweck muss jeder EU-Mitgliedstaat jeweils einen Umsetzungsrechtsakt erlassen. Aus diesem Grund verfehlte die EG-Datenschutzrichtlinie schließlich ihr Ziel der Angleichung des Datenschutzniveaus innerhalb der EU: es bildeten sich zwischen den EU-Mitgliedstaaten unterschiedliche Datenschutz-Regime heraus, welche sich aus den jeweils verabschiedeten nationalen Umsetzungsgesetzen ergaben. Datenverarbeitungstätigkeiten, die in einem EU-Mitgliedstaat rechtskonform waren, konnten in einem anderen Mitgliedstaat im Hinblick auf die spezifische Ausführung der Datenverarbeitung rechtswidrig sein.

1.1.2 Die Datenschutz-Grundverordnung

Im Jahr 2016 verabschiedete der europäische Gesetzgeber die Datenschutz-Grundverordnung, welche die EG-Datenschutzrichtlinie von 1995 ab Mai 2018 ersetzt. Sie ist das Ergebnis eines schwierigen und langen Verhandlungsprozesses, der aufgrund zahlloser Änderungsvorschläge zum Gesetzestext vier Jahre bis zur Verabschiedung der endgültigen Verordnung in Anspruch nahm.

Die aufgezeigte Fragmentierung des Datenschutzes innerhalb der EU-Mitgliedstaaten und die daraus resultierenden Rechtsunsicherheiten wurden als Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten angesehen und führten zu Wettbewerbsverzerrungen.⁵ Im Gegensatz zur EG-Datenschutzrichtlinie ist die Datenschutz-Grundverordnung deshalb *direkt anwendbar* – Umsetzungsrechtsakte aufseiten der EU-Mitgliedstaaten sind nicht mehr erforderlich. Durch die so erzeugte Angleichung der Datenschutzvorschriften soll die DSGVO zu mehr Rechtssicherheit innerhalb der EU führen und Hindernisse für den grenzüberschreitenden Austausch personenbezogener Daten beseitigen.

³ Polenz, in: Kilian/Heussen, Computerrechts-Handbuch, Grundbegriffe (2013), Rn. 3

⁴ ErwGr. 3 DSGVO

⁵ ErwGr. 9 DSGVO

Die EU möchte mit der DSGVO das Vertrauen der Bürger zurückgewinnen, indem über die Schaffung eines einheitlichen Rechtsrahmens ein verantwortungsbewusster Umgang mit ihren personenbezogenen Daten sichergestellt werden soll. Auf dieser Grundlage möchte der europäische Gesetzgeber eine Förderung der digitalen Wirtschaft im europäischen Binnenmarkt erreichen.⁶ Unternehmen treffen zudem nach der DSGVO neue Datenschutzpflichten, gleichzeitig werden bereits bestehende datenschutzrechtliche Verpflichtungen verschärft. Der europäische Gesetzgeber hat unter Berücksichtigung der Herausforderungen der globalen Wirtschaft, neuer Technologien sowie neuer Geschäftsmodelle für die Verordnung einen äußerst weiten Anwendungsbereich vorgesehen. Schließlich wurden nicht nur die datenschutzrechtlichen Pflichten, sondern auch der Bußgeldrahmen signifikant erhöht. Daher sollten Unternehmen ihre datenschutzrelevanten Verarbeitungsprozesse einer sorgfältigen Prüfung unterziehen und gegebenenfalls Anpassungen vornehmen, um sie in Einklang mit den Vorgaben der DSGVO zu bringen.

1.1.3 Das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU

Die DSGVO ist als Verordnung in allen ihren Teilen verbindlich und gilt ohne mitgliedstaatlichen Umsetzungsakt unmittelbar.⁷ Damit verbleibt den nationalen Gesetzgebern im Anwendungsbereich der DSGVO grundsätzlich keine Regelungsmöglichkeit. Allerdings lässt die DSGVO über *zahlreiche Öffnungsklauseln* den EU-Mitgliedstaaten Raum zur Schaffung ergänzender nationaler Regelungen. Dadurch wird es auch zukünftig nationale Besonderheiten im Datenschutzrecht geben.

Als erster EU-Mitgliedstaat hat Deutschland von diesem Gestaltungsspielraum Gebrauch gemacht und bereits im November 2016 – wenige Monate nach Verabschiedung der DSGVO – den ersten Entwurf für ein deutsches Gesetz zur Umsetzung der Verordnung vorgelegt.⁸ Das Gesetz dient nicht nur der Ausfüllung des gesetzgeberischen Spielraums gemäß der Öffnungsklauseln der DSGVO sondern zugleich der Umsetzung der Richtlinie (EU) 2016/680 zum Datenschutz in Strafsachen.⁹

⁶ErwGr. 7, 9 DSGVO

⁷Ruffert, in: Calliess/Ruffert, EUV/AEUV, Art. 288 AEUV (2016) Rn. 19 f.; St. Rspr. bspw. EuGH, Entscheidung vom 14. Dezember 1971, Politi/Finanzministerium Italien, Rs. 43/71, ErwGr. 9; EuGH, Entscheidung vom 17. Mai 1972, Orsolina Leonesio./Italien, ErwGr. 5 f.

⁸Die österreichische Regierung veröffentlichte Anfang Juni 2017 ihren ersten Entwurf für ein Datenschutz-Anpassungsgesetz. Aktuelle Informationen zum Gesetzgebungsverfahren sind verfügbar unter <https://www.help.gv.at/Portal.Node/hlpd/public/content/171/Seite.1710942.html>, zuletzt aufgerufen am 14. Juni 2017

⁹Richtlinie (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 Zweck 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

Das *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU* (nachfolgend *kurz*: BDSG-neu) ersetzt das alte BDSG (*kurz*: BDSG-alt) und tritt im Gleichlauf mit der DSGVO am 25. Mai 2018 in Kraft.¹⁰ Infolge kritischer Stimmen zum Entwurf wurden entsprechende Änderungsvorschläge im Laufe des Gesetzgebungsverfahrens eingearbeitet.¹¹ Das BDSG-neu wurde schließlich am 27. April 2017 vom Bundestag beschlossen und der Bundesrat stimmte dem Gesetz am 12. Mai 2017 zu. Inwieweit die Regelungen insgesamt mit dem Europarecht, insbesondere der DSGVO, vereinbar sind, wird sich in naher Zukunft zeigen. Die Kritik an den beschlossenen Regelungen hält auch nach dem Inkrafttreten an.¹²

1.2 Checkliste – Die wichtigsten datenschutzrechtlichen Pflichten

Für einen kursorischen Überblick über die datenschutzrechtlichen Pflichten nach der DSGVO fasst die nachfolgende „Checkliste“ die *wichtigsten Pflichten* für datenverarbeitende Unternehmen zusammen. Zudem enthält die Liste Verweise auf die entsprechenden Kapitel und Abschnitte dieses Handbuchs.

1.2.1 Datenschutzorganisation

Unternehmen werden erhebliche Anstrengungen unternehmen müssen, um ihre interne Datenschutzorganisation in Einklang mit den Anforderungen der DSGVO zu bringen. Diverse organisatorische Verpflichtungen sind künftig zu erfüllen.

Verzeichnis von Verarbeitungstätigkeiten

Verantwortliche und Auftragsverarbeiter müssen Verzeichnisse über ihre Verarbeitungstätigkeiten führen. Diese sollen – soweit sie ordnungsgemäß umgesetzt und aufrechterhalten werden – den Nachweis der Umsetzung der Vorgaben der DSGVO gegenüber den Aufsichtsbehörden ermöglichen und zudem bei der Erfüllung von Informationspflichten gegenüber den betroffenen Personen als Hilfsmittel dienen. Die Verzeichnisse müssen unter anderem Informationen zum Verarbeitungszweck, den Kategorien der verarbeiteten personenbezogenen Daten sowie eine Beschreibung der eingesetzten technischen und organisatorischen Schutzmaßnahmen enthalten. [Abschn. 3.4](#) enthält detaillierte Informationen zu Inhalt und Zweck der Verzeichnisse sowie zu den – in der Praxis selten anwendbaren – Ausnahmen von dieser datenschutzrechtlichen Pflicht.

¹⁰ Art. 8 Abs. 1 BDSG-neu

¹¹ Bundesrat (2017) Beschlussdrucksache 110/17(B); Deutscher Bundestag (2017a) Beschlussempfehlung; kritisch Zimmer-Helfrich, ZD 2017, 51, 51 ff.; Helfrich, ZD 2017, 97, 98; Deutscher Bundestag. Online-Dienste (2017b) Kritik

¹² Krempf (2017) Datenschutzreform; ZD-Aktuell 2017, 05637; Helfrich, ZD 2017, 97, 98

Benennung eines Datenschutzbeauftragten

Privatunternehmen sind zur Ernennung eines Datenschutzbeauftragten verpflichtet, soweit ihre Kerntätigkeit – also Tätigkeiten, die für die Umsetzung der Geschäftsstrategie maßgeblich sind – in der Durchführung von Verarbeitungstätigkeiten besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (bspw. Gesundheitsdaten) besteht. Hinzu kommen im nationalen Kontext nach dem BDSG-neu weitere Fälle, die eine Benennungspflicht auslösen. Unternehmensgruppen steht es frei für alle oder mehrere Gruppenunternehmen einen gemeinsamen Datenschutzbeauftragten zu benennen. Der Datenschutzbeauftragte ist anhand seiner Expertise und beruflichen Qualifikation auszuwählen. Dadurch soll sichergestellt werden, dass er seine Pflichten ordnungsgemäß erfüllen kann, wie z. B. die Überwachung der Einhaltung der Vorschriften der DSGVO durch das Unternehmen. Nähere Ausführungen finden sich in [Abschn. 3.6](#).

Datenschutz-Folgenabschätzung

Sollte eine geplante Verarbeitungstätigkeit, insbesondere unter Verwendung neuer Technologien, zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führen, müssen Unternehmen eine präventive Datenschutz-Folgenabschätzung vornehmen, um geeignete Maßnahmen zur Minimierung des Datenschutzrisikos zu ermitteln. Das Unternehmen konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus dieser Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Zudem erstellen und veröffentlichen die Aufsichtsbehörden künftig Listen von Verarbeitungsvorgängen (sog. „black- and whitelists“), für die eine Datenschutz-Folgenabschätzung erforderlich oder nicht erforderlich ist. Für Details zum Umfang der Datenschutz-Folgenabschätzung, sowie zu den betroffenen Verarbeitungstätigkeiten siehe [Abschn. 3.5](#).

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Die DSGVO legt einen Schwerpunkt auf präventive Datenschutzkonzepte. Da die Verpflichtung zur Berücksichtigung und Umsetzung der Prinzipien von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bußgeldbewährt ist, sollten sich Unternehmen dieser Themen ernsthaft annehmen, siehe [Abschn. 3.7](#). Dies gilt insbesondere für solche Unternehmen, deren Kerntätigkeiten in der Verarbeitung großer Mengen personenbezogener Daten bestehen, siehe dazu [Abschn. 9.1](#).

Technischer und organisatorischer Datenschutz

Unternehmen müssen technische und organisatorische Datenschutzmaßnahmen treffen, um die Sicherheit der von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten. Das angemessene Datenschutzniveau ist im konkreten Fall anhand

des Risikopotenzials der jeweiligen Datenverarbeitungstätigkeiten zu ermitteln. Einzelheiten zur Bestimmung des Risikopotenzials sowie zu den angemessenen Datenschutzmaßnahmen werden in [Abschn. 3.3](#) dargelegt.

Rechte betroffener Personen

Betroffene Personen haben umfangreiche Informationsrechte gegenüber datenverarbeitenden Unternehmen. Letztere müssen proaktiv zahlreiche Pflichten gegenüber den betroffenen Personen erfüllen, wie etwa die Erteilung von Informationen über die Verarbeitung, das Löschen von personenbezogenen Daten oder die Berichtigung unvollständiger personenbezogener Daten. Vor allem das neu eingeführte Recht auf Datenübertragbarkeit wird Unternehmen vor Herausforderungen stellen, da sie ihren Kunden auf Anfrage deren Datensätze in einem interoperablen Format zur Verfügung stellen müssen. Die Einzelheiten zu den verschiedenen Betroffenenrechten sind in [Kap. 4](#) dargestellt.

Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

Die DSGVO führt eine allgemeine Meldepflicht der Verantwortlichen gegenüber den Aufsichtsbehörden für Datenschutzverletzungen (sog. „data breach notifications“) ein. Eine Datenschutzverletzung kann u. a. zur Vernichtung, zum Verlust oder zur unbefugten Offenlegung von personenbezogenen Daten führen. Die Meldung gegenüber den Aufsichtsbehörden muss regelmäßig innerhalb eines Zeitraums von 72 Stunden nach Bekanntwerden der Verletzung erfolgen. Im Falle eines Zwischenfalls mit hohem Risiko für die Rechte und Freiheiten der betroffenen Personen hat der Verantwortliche die Verletzung zusätzlich auch den betroffenen Personen mitzuteilen. In einem derartigen Fall werden die Aufsichtsbehörden den Verantwortlichen bei der Kommunikation unterstützen. Die Einzelheiten werden in [Abschn. 3.8](#) dargestellt.

Datenschutzmanagement

Soweit auf Grundlage des Budgets und der Ressourcen eines Unternehmens möglich, kann die Einhaltung der Vorgaben der DSGVO mithilfe eines Datenschutz-Managementsystems sichergestellt und überwacht werden. Dabei handelt es sich um ein internes Compliance-System, welches die Erfüllung datenschutz- und sicherheitsbezogener Pflichten überprüft, siehe [Abschn. 3.2.1](#). Ein Vier-Phasen-Plan zur praktischen Implementierung eines solchen Systems wird in [Kap. 10](#) dargestellt.

Benennung eines Vertreters durch nicht in der EU niedergelassene Unternehmen

Unternehmen, auf die die DSGVO Anwendung findet, obwohl sie keine Niederlassung in der EU haben, müssen einen Vertreter in der EU benennen. Dieser soll als Anlaufstelle für betroffene Personen und Aufsichtsbehörden dienen, siehe [Abschn. 4.3.8](#).

Verhaltensregeln & Datenschutzzertifizierungen

Auch wenn deren Verwendung nicht verpflichtend ist, weist die DSGVO Selbstregulierungsinstrumenten, wie Verhaltensregeln und Datenschutzzertifizierungen,

eine erhöhte praktische Relevanz zu. Während Verhaltensregeln die Verpflichtungen der DSGVO für einen bestimmten Sektor oder eine bestimmte Technologie präzisieren, dienen Datenschutzzertifizierungen dem Nachweis der Einhaltung der Vorgaben der DSGVO bzgl. der zertifizierten Verarbeitungstätigkeiten. Die Verwendung dieser Instrumente erleichtert den Nachweis der Einhaltung der DSGVO gegenüber den Aufsichtsbehörden, [Abschn. 3.9](#). Zudem können Unternehmen diese Instrumente als geeignete Datenschutz-Garantien für Datentransfers in Drittländer nutzen, siehe [Abschn. 4.3.6](#).

1.2.2 Rechtmäßigkeit der Datenverarbeitung

Zusätzlich zu ihren organisatorischen Verpflichtungen nach der DSGVO müssen Unternehmen die materielle Rechtmäßigkeit ihrer Datenverarbeitungsvorgänge sicherstellen. Dies betrifft auch konzerninterne Datenverarbeitungen, sowie Datentransfers in Drittländer und Verarbeitungstätigkeiten unter Einbeziehung eines Auftragsverarbeiters.

Rechtsgrundlagen für die Verarbeitung

Datenverarbeitungstätigkeiten unterliegen einem generellen Verbot mit Erlaubnisvorbehalt. Die meisten der in der DSGVO vorgesehenen Rechtsgrundlagen für eine Verarbeitung waren bereits in der EG-Datenschutzrichtlinie enthalten. Die Voraussetzungen für die Einholung einer wirksamen Einwilligung der betroffenen Personen in die Datenverarbeitung wurden verschärft, wie in [Abschn. 4.2.1](#) dargestellt. Andere gesetzliche Erlaubnistatbestände sind, unter anderem, die Notwendigkeit der Verarbeitung zur Vertragserfüllung oder die überwiegenden berechtigten Interessen des Verantwortlichen an der Datenverarbeitung. Zudem sollten sich Unternehmen bewusst machen, dass eine Änderung des Verarbeitungszwecks nur in begrenzten Fällen zulässig ist. Einzelheiten werden in [Abschn. 4.2.2.5](#) dargestellt.

Konzerninterne Datenverarbeitungen

Die DSGVO sieht kein Konzernprivileg vor, sodass jedes Konzernunternehmen selbst für die Einhaltung der datenschutzrechtlichen Standards im Rahmen seiner Verarbeitungstätigkeiten verantwortlich ist. Deshalb müssen auch konzerninterne Datentransfers von einer Rechtsgrundlage gedeckt sein, grundsätzlich im gleichen Maß wie jeder Datentransfer an sonstige Dritte, siehe [Abschn. 4.4](#).

Besondere Kategorien personenbezogener Daten

Besondere Kategorien von personenbezogenen Daten beziehen sich, unter anderem, auf die politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen oder die Gesundheit der betroffenen Personen. Diese Daten sind besonders schutzwürdig und ihre Verarbeitung kann nur unter Einsatz angemessener Schutzmaßnahmen erfolgen, die dem hohen Risikopotenzial der Verarbeitungssituation entsprechen. Da Beschäftigendaten unter Umständen auch Informationen zur Gesundheit von Mitarbeitern enthalten, werden Unternehmen von diesen Einschränkungen

regelmäßig betroffen sein. Dabei müssen sie beachten, dass die Verarbeitung besonderer Kategorien personenbezogener Daten verboten ist, soweit diese nicht durch die Einwilligung der betroffenen Personen oder durch die Notwendigkeit der Verarbeitung in einem Arbeits- oder Sozialversicherungskontext gerechtfertigt ist. Einzelheiten zu den verschiedenen Arten besonderer Kategorien personenbezogener Daten sowie zu den rechtlichen Grundlagen für ihre Verarbeitung sind [Abschn. 4.2.3](#) zu entnehmen.

Auftragsverarbeitung

Die DSGVO qualifiziert den Auftragsverarbeiter nicht als Dritten. Deshalb liegt die Weitergabe personenbezogener Daten an einen Auftragsverarbeiter im freien Ermessen des Verantwortlichen und bedarf keines eigenen materiell-rechtlichen Erlaubnistatbestandes. Es ist zu beachten, dass dies auch für die Beteiligung von Auftragsverarbeitern außerhalb der EU gilt. Nichtsdestotrotz ist der Verantwortliche zur Auswahl eines geeigneten Auftragsverarbeiters verpflichtet, welcher ein angemessenes Datenschutzniveau gewährleisten kann. In diesem Zusammenhang treffen den Auftragsverarbeiter auch eigene, bußgeldbewährte Pflichten nach der DSGVO. Einzelheiten werden in [Abschn. 3.10](#) dargestellt.

Generelle Anforderungen an Datenübermittlungen in Drittländer

Werden personenbezogene Daten an Empfänger außerhalb der EU übermittelt, muss dieser Transfer bestimmten Garantien entsprechen, um ein angemessenes Datenschutzniveau beim Empfänger zu gewährleisten. Unternehmen müssen in zwei Stufen sicherstellen, dass die Verarbeitungstätigkeit (i) von einer Rechtsgrundlage gedeckt ist und (ii) dass der Transfer vom Empfänger einzuhaltenden Garantien unterliegt. Die verschiedenen Garantiemechanismen sind in [Abschn. 4.3](#) beschrieben. Aus Unternehmenssicht von hoher praktischer Relevanz sind:

EU-Standardvertragsklauseln Der in der EU niedergelassene Datenexporteur und der außerhalb der EU niedergelassene Datenimporteur können einen Vertrag auf der Grundlage von Standarddatenschutzklauseln (sog. EU-Standardvertragsklauseln) schließen. Dabei handelt es sich um Sets von Vertragsklauseln, die von der Europäischen Kommission oder einer der nationalen Aufsichtsbehörden verabschiedet werden. Werden die Klauseln vollständig und unverändert übernommen, dienen sie als ausreichende Garantiemaßnahme für internationale Datentransfers, siehe [Abschn. 4.3.3](#) für Einzelheiten.

EU-U.S. Privacy Shield Datentransfers in die USA, die in Konzernstrukturen häufig stattfinden, können auf Grundlage des EU-U.S. Privacy Shields erfolgen. Dabei handelt es sich um einen Rechtsakt, der von der Europäischen Kommission verabschiedet wurde. Er ermöglicht U.S.-Unternehmen eine (Selbst-)Zertifizierung bzgl. der Einhaltung eines angemessenen Datenschutzniveaus. Die Privacy Shield-Prinzipien sowie seine Wirkungsweise und ein Ausblick auf jüngere rechtliche Entwicklungen sind in [Abschn. 4.3.4](#) dargestellt.

Binding Corporate Rules Konzerne oder Gruppen von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, können sich als geeignete Garantien Binding Corporate Rules auferlegen. Diese legen für die beteiligten Unternehmen eine weltweite Datenschutz-Policy im Hinblick auf Datentransfers zu Gruppenmitgliedern in Empfängerländern außerhalb der EU fest, die kein hinreichendes Datenschutzniveau vorweisen können. Ihre Wirkungsweise, ihr Mindestinhalt sowie das einzuhaltende Genehmigungsverfahren sind in [Abschn. 4.3.5](#) beschrieben.

Referenzen

- Bundesrat (2017) Beschlussdrucksache 110/17(B)
- Deutscher Bundestag (2017a) Beschlussempfehlung des Innenausschusses, Drucksache 18/12084
- Deutscher Bundestag. Online-Dienste (2017b) Kritik von Sachverständigen an geplanter Datenschutz-Novelle. <https://www.bundestag.de/dokumente/textarchiv/2017/kw13-pa-innen-datenschutz/499054>. Zugegriffen: 13. Juni 2017
- Helfrich M (2017) DSAnpUG-EU: Ist der sperrige Name hier schon Programm? S 97–98
- Krempel S (2017) Datenschutzreform: EU-Kommission droht Deutschland mit Vertragsverletzungsverfahren. <https://www.heise.de/newsticker/meldung/Datenschutzreform-EU-Kommission-droht-Deutschland-mit-Vertragsverletzungsverfahren-3689759.html>. Zugegriffen: 13. Juni 2017
- Martini M (2017) Art. 25 DSGVO. In: Paal BP, Pauly DA (Hrsg) Beck'sche Kompaktcommentare Datenschutz-Grundverordnung, 1. Aufl. C.H. Beck, München
- Polenz S (2013) Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes. In: Kilian W, Heussen B (Hrsg) Computerrechts-Handbuch, Stand 8/2013. C.H. Beck, München
- Reiners W (2015) Datenschutz in der Personal Data Economy – Eine Chance für Europa. ZD 5(2):51–55
- Ruffert M (2016) Art. 288 AEUV. In: Calliess C, Ruffert M (Hrsg) EUV/AEUV, 5. Aufl. C.H. Beck, München
- Zimmer-Helfrich A (2017) BDSG-neu: BMI-Entwurf für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU, Interview. ZD 7(2):51–54

Die Einhaltung der Vorgaben der DSGVO wird den betroffenen Unternehmen eine regelmäßig zeit- und kostenintensive Überprüfung ihrer bisherigen Datenschutzstandards abverlangen. Deshalb sollten Unternehmen zunächst prüfen, ob sie vom Inkrafttreten der DSGVO betroffen sind, also ob die Verordnung überhaupt auf sie Anwendung findet.

2.1 In welchen Fällen ist die Verordnung anwendbar? – sachlicher Anwendungsbereich

Artikel 2 – Sachlicher Anwendungsbereich

1. Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

[...]

Vereinfacht gesagt umfasst der sachliche Anwendungsbereich der DSGVO *jegliche Verarbeitungen personenbezogener Daten*. Die Verordnung wird daher für Unternehmen relevant, sobald sie Verarbeitungstätigkeiten jedweder Art vornehmen. Der (sachliche) Anwendungsbereich ist *sehr weit zu interpretieren*, um ein hohes Schutzniveau zu gewährleisten.

2.1.1 „Verarbeitung“

„Verarbeitung“ bezieht sich auf jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten *Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten*, Art. 4 Nr. 2 DSGVO. Jeder Umgang mit Daten wird praktisch

von dieser Definition erfasst. Beispiele sind das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Löschen oder die Vernichtung von Daten. Der offene Wortlaut ergibt sich aus dem Ziel des europäischen Gesetzgebers, den Anwendungsbereich unabhängig von technologischen Veränderungen bestimmen zu können.¹ Er umfasst sowohl Verarbeitungen, die *ganz als auch teilweise mithilfe automatisierter Verfahren* durchgeführt werden, wobei sich letzteres auf Verarbeitungen bezieht, bei denen bestimmte Verarbeitungsschritte von natürlichen Personen ausgeführt werden, z. B. durch die Erfassung von Daten in einem Computersystem.²

Beispiel

- Personenbezogene Daten werden durch den Einsatz von Computern, Smartphones, Webcams, Dashcams oder Kameradrohnen verarbeitet
- Personenbezogene Daten werden mittels Wearables oder anderer smart devices (z. B. Smart Cars) erhoben³

Die offene Definition der „Verarbeitung“ umfasst auch kurzzeitige Nutzungen kleiner Datenmengen.⁴

Beispiel

- Personenbezogene Daten werden von einem IT-System zwischengespeichert, wie z. B. im Verlauf eines Browsers
- Personenbezogene Daten werden auf einem Computerbildschirm angezeigt

Manuelle Datenverarbeitung

Ausgehend von der Legaldefinition ist auch die manuelle Datenverarbeitung als „Verarbeitung“ i. S. d. DSGVO anzusehen. Im Gegensatz zu automatisierten Verarbeitungsvorgängen unter Einsatz von Technologie wird die manuelle Verarbeitung *vollständig von Menschen ausgeführt* – ohne Einsatz von Maschinen oder anderen Werkzeugen. Naturgemäß verlaufen diese Tätigkeiten wesentlich langsamer als automatisierte Verarbeitungsvorgänge, sodass deutlich geringere Datenmengen verarbeitet werden können. Deshalb unterfallen manuelle Datenverarbeitungen der DSGVO nur, wenn *zwei Bedingungen* erfüllt sind:

- Die betroffenen Daten müssen in einem *Dateisystem* gespeichert sein oder sollen dort gespeichert werden (Art. 2 Abs. 1 DSGVO). Ausgehend von vorbestimmten Ordnungskriterien werden Daten in einem Dateisystem in verschiedene Gruppen eingeteilt und systematisch verwaltet; und

¹ ErwGr. 15 DSGVO

² Ernst: in: Paal/Pauly, DSGVO, Art. 2 (2017), Rn. 6

³ Beispiele aus Ernst, in: Paal/Pauly, DSGVO, Art. 2 (2017), Rn. 5–6

⁴ Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016) Rn. 10, siehe auch für die nachfolgenden Beispiele

- Die verschiedenen Datengruppen müssen *anhand vorbestimmter Kriterien geordnet* sein.⁵ Die Verordnung gibt keine Voraussetzungen bzgl. dieser Kriterien vor.

Ausgehend von den unter der alten Rechtslage relevanten Kriterien und der weiten Interpretation der DSGVO sollten bspw. chronologisch, alphabetisch oder anhand anderer Kriterien geordnete Akten diese Bedingungen erfüllen.⁶

Beispiel

Eine Arztpraxis speichert ihre Patientendaten in Papierakten. Diese Akten sind alphabetisch anhand der Nachnamen der Patienten in mehreren Aktenschränken sortiert. Es gibt bspw. eine Schublade für alle Nachnamen, die mit „A“ beginnen, eine für alle Nachnamen die mit „B“ beginnen und so weiter.

In diesem Beispiel sind die Patientendaten alphabetisch sortiert. Dadurch sind die Daten in einem Dateisystem anhand festgelegter Kriterien gespeichert und fallen somit in den sachlichen Anwendungsbereich der DSGVO.

2.1.2 „Personenbezogene Daten“

Wie soeben dargelegt fällt jeder systematische Umgang mit Daten unter den Begriff der „Verarbeitung“ i.S.d. DSGVO.⁷ Der Begriff „Daten“ bezieht sich auf Informationen bzw. Einzelangaben.⁸ Außerdem müssen die Daten „personenbezogen“ sein, um in den Anwendungsbereich der Verordnung zu fallen. Daten haben einen Personenbezug, soweit sie sich auf eine *identifizierte oder identifizierbare natürliche Person* beziehen, Art. 4 Nr. 1 DSGVO. Sie fallen also in den Anwendungsbereich der Verordnung, sobald die Identifizierung einer Person aufgrund der vorhandenen Daten möglich ist, was bedeutet, dass eine Person direkt oder indirekt mittels Zuordnung zu einem Kennungsmerkmal ermittelt werden kann. Dies ist der Fall, sobald die *Zuordnung der Daten zu einem oder mehreren Charakteristika*, die Ausdruck der physischen, physiologischen, psychischen, genetischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, möglich ist. Dabei kann es sich bspw. handeln um:

- Den Namen einer Person⁹;
- Identifikationsnummern, wie Sozialversicherungsnummer, Personalnummer oder Personalausweisnummer;

⁵ ErwGr.15 DSGVO

⁶ Plath, in: Plath, BDSG/DSGVO, Art. 2 DSGVO (2016), Rn. 7

⁷ Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), Rn. 7

⁸ Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), Rn. 3; siehe auch Dammann, in: Simitis, BDSG, § 3 (2014), Rn. 4–6

⁹ Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), Rn. 8

- Standortdaten;
- Online-Kennungen (dies kann IP-Adressen oder Cookies einschließen¹⁰).

Die DSGVO ist *nicht* auf die *Daten Verstorbener* anwendbar.¹¹ Hierbei ist aber zu beachten, dass es sich bei derartigen Daten zugleich um die personenbezogenen Daten eines lebenden Verwandten oder Nachkömmlings des Verstorbenen handeln kann.¹² Solche Daten können bspw. Aufschluss über Erbkrankheiten von Nachkommen des Verstorbenen liefern.¹³ In diesem Fall unterfallen sie dem Anwendungsbereich der DSGVO.

2.1.2.1 Identifizierbarkeit der betroffenen Person

Wie soeben erwähnt, muss die Identifizierung der betroffenen Person nicht unmittelbar anhand der Daten möglich sein, um zur Anwendbarkeit der DSGVO zu führen. Die bloße Möglichkeit der Identifizierung, also die „Identifizierbarkeit“, stellt bereits einen hinreichenden Personenbezug der Daten i. S. d. DSGVO her. Die Identifizierung wird dabei erst durch die *Kombination verschiedener Informationen* möglich, die für sich allein keinen Rückschluss auf den Betroffenen zugelassen hätten, aber einen solchen in der Zusammenschau ermöglichen. Der Wortlaut des Art. 4 Nr. 1 DSGVO lässt offen, wer zur Identifizierung der betroffenen Person in der Lage sein muss, was darauf hindeutet, dass zusätzliche Informationen für die Identifizierung nicht zwingend im Datenbestand des Verantwortlichen/Auftragsverarbeiters vorhanden sein müssen.

Relative Kriterien

Unter der EG-Datenschutzrichtlinie waren zur Bestimmung der Wahrscheinlichkeit einer Identifizierbarkeit alle Mittel zu berücksichtigen, die vom Verantwortlichen oder einem Dritten vernünftigerweise zum Erhalt zusätzlicher Informationen eingesetzt werden konnten (ErwGr. 26 EG-Datenschutzrichtlinie). In diesem Zusammenhang wurde allerdings kontrovers diskutiert, ob relative oder absolute Kriterien zur *Feststellung der vernünftigerweise bestehenden Wahrscheinlichkeit* heranzuziehen sind.¹⁴ Die Verwendung absoluter Kriterien würde dazu führen, dass die Definition „personenbezogener Daten“ bereits erfüllt ist, sobald *irgendjemand die Möglichkeit zur Zuordnung* der verarbeiteten Daten zu einer natürlichen Person hat.¹⁵ Im Oktober 2016 entschied der EuGH, dass das tatsächliche Identifikationsrisiko unwesentlich erscheint, wenn die Zuordnung der Daten zu einem Individuum einen unverhältnismäßigen Aufwand in Bezug auf Zeit, Kosten und Personaleinsatz

¹⁰ ErwGr. 30 DSGVO

¹¹ ErwGr. 27 DSGVO

¹² Ernst, in: Paal/Pauly, DSGVO, Art. 4 (2017), Rn. 6; Schild, in: Wolff/Brink, BeckOK, Art. 4 DSGVO (2016), Rn. 5; siehe auch Dammann, in: Simitis, BDSG, § 3 (2014), Rn. 17

¹³ Siehe auch Dammann, in: Simitis, BDSG, § 3 (2014), Rn. 17

¹⁴ Für Literaturangaben zu beiden Ansichten, siehe Voigt, MMR 2009, 377, 378 ff.; Bergt, ZD 2015, 365, 365 ff.

¹⁵ Siehe auch Herbst, NVwZ 2016, 902, 904

erfordert, wobei es sich bei den vorgenannten Faktoren um *relative Kriterien* handelt.¹⁶ Wenn also die Identifizierung des Betroffenen für den Verantwortlichen/Auftragsverarbeiter ausgehend von seiner Möglichkeit zum Zugriff auf zusätzliche Informationen ohne unverhältnismäßigen Aufwand möglich ist, gelten die Daten als „personenbezogene Daten“. Auch wenn das Urteil des EuGH auf Grundlage der EG-Datenschutzrichtlinie ergangen ist, enthält die DSGVO Indikatoren dafür, dass relative Kriterien auch weiterhin Anwendung finden werden.¹⁷ Daher gilt eine Person als identifizierbar, wenn die *fehlenden Informationen*, welche eine Identifizierung ermöglichen, (*leicht*) *zugänglich* sind, beispielsweise weil sie im Internet oder von einem (kommerziellen) Informationsdienst veröffentlicht wurden. Auch die Kenntnis Dritter von diesen Informationen ist zu berücksichtigen, sobald eine Chance besteht, dass der Verantwortliche/Auftragsverarbeiter Zugriff auf dieses Wissen erhält. So können von einem Verantwortlichen gespeicherte dynamische IP-Adressen personenbezogene Daten der betroffenen Person sein, sofern dem Verantwortlichen bspw. rechtliche Mittel zur Verfügung stehen, die vernünftigerweise eingesetzt werden können, um mithilfe Dritter (Internetzugangsanbietern oder zuständigen Behörden) die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.¹⁸ Im Umkehrschluss: sobald keine realistische Chance besteht, dass der Verantwortliche/Auftragsverarbeiter Zugriff auf die Information erlangt, gilt eine Person nicht als identifizierbar.

Umstände des Einzelfalls

Um eine Identifizierbarkeit zu beurteilen sind des Weiteren die Umstände des Einzelfalls zu berücksichtigen. Dies bezieht sich u. a. auf¹⁹:

- Die für die Identifizierung notwendigen *zeitlichen und monetären Mittel*;
- Die zum Verarbeitungszeitpunkt verfügbare Technologie sowie *technologische Entwicklungen*;
- Der *Zweck der Verarbeitung*.

Die Verpflichtung zur Berücksichtigung technologischer Entwicklungen könnte sich in der Praxis als Herausforderung erweisen, da sie vorsieht, dass Verantwortliche/Auftragsverarbeiter die absehbaren oder wahrscheinlichen Entwicklungen in ihre Beurteilung einfließen lassen müssen.²⁰ Ist der Verarbeitungszweck nur über

¹⁶ EuGH, Entscheidung vom 19. Oktober 2016, Breyer/Bundesrepublik Deutschland, C-582/14, ErwGr. 46

¹⁷ Hiermit ist beispielsweise ErwGr. 26 DSGVO gemeint, der die Worte „sollten alle Mittel berücksichtigt werden, die [...] nach allgemeinem Ermessen wahrscheinlich genutzt werden“ und „sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden“ verwendet; zustimmend siehe Piltz, K&R 2016, 557, 561; Barlag, in: Roßnagel, DSGVO, Anwendungsbereich (2017), Rn. 9 ff.; Schreiber, in: Plath, BDSG/DSGVO, Art. 4 DSGVO (2016), Rn. 9; ablehnend siehe Buchner, DuD 2016, 155, 156

¹⁸ BGH, Urteil vom 16. Mai 2017, Breyer, VI ZR 135/13, S. 10

¹⁹ ErwGr. 26 DSGVO

²⁰ Piltz, K&R 2016 557, 561

eine Identifikation der betroffenen Personen erreichbar, kann unterstellt werden, dass der Verantwortliche/Auftragsverarbeiter über die Mittel zur Identifizierung dieser Betroffenen verfügt.²¹ Kurz gesagt, je einfacher und schneller eine natürliche Person ermittelt werden kann, desto eher handelt es sich um eine „identifizierbare natürliche Person“.

2.1.2.2 Anonymisierung und Pseudonymisierung

Anonymisierung

Anonymisierung ist eine Technik zur *Veränderung* personenbezogener Daten mit dem Ergebnis, dass *keine Verbindung* der Daten zu einer natürlichen Person (mehr) besteht. Anonymisierte Daten sind Informationen, die entweder keinen Bezug zu einer identifizierten oder identifizierbaren Person haben, oder es handelt sich um personenbezogene Daten, bei denen der Personenbezug aufgrund einer durchgeführten Anonymisierung nicht mehr besteht.²² Die Anonymisierung kann durch eine Reihe verschiedener *Techniken* erreicht werden, die in der Regel in eine der *beiden nachfolgenden Kategorien* fallen:

1. *Randomisierung*: Diese Technik besteht in der Veränderung der Genauigkeit von Daten, um die starke Verbindung zwischen den Daten und der betroffenen Person zu entfernen. Werden die Daten hinreichend ungenau bzw. unzuverlässig, können sie nicht mehr einer bestimmten Person zugeordnet werden.²³
2. *Verallgemeinerung*: Diese Technik besteht in der Verallgemeinerung/Verwässerung der Merkmale der betroffenen Personen, indem der entsprechende Bezugspunkt oder die Reihenfolge der Daten verändert wird (z. B. Bezug der Daten zu einer Region anstelle einer Stadt, zu einem Monat anstelle einer Woche).²⁴

Im Falle einer erfolgreichen Anonymisierung ist die *DSGVO nicht anwendbar*.²⁵ Derartige Techniken werden häufig im Zusammenhang mit statistischen oder Forschungszwecken angewandt. Sobald der Verantwortliche/Auftragsverarbeiter die anonymisierten Informationen allerdings mit hinreichender Wahrscheinlichkeit wiederherstellen kann, handelt es sich um personenbezogene Daten im Anwendungsbereich der DSGVO.

Beispiel

Für sein anstehendes zwanzigstes Jubiläum möchte ein privater Nachhilfeeinbieter herausfinden, wie viele seiner bisher betreuten Schüler eine Universität besucht haben und, sofern dies der Fall war, was sie studiert haben. Zu diesem

²¹ Siehe auch Art.-29-Datenschutzgruppe, WP 136 (2007), S. 19 ff.

²² ErwGr. 26 DSGVO

²³ Siehe auch Art.-29-Datenschutzgruppe, WP 216 (2014), S. 12

²⁴ Siehe auch Art.-29-Datenschutzgruppe, WP 216 (2014), S. 16

²⁵ ErwGr. 26 DSGVO

Zweck erhebt der Anbieter die Daten seiner Nachhilfeschüler der vergangenen 20 Jahre und kontaktiert diese via E-Mail, in welcher um die Teilnahme an einer Online-Befragung gebeten wird. Um die Daten der betroffenen Personen zu anonymisieren enthält die Umfrage keine Fragen zu Namen, E-Mail-Adressen, Abschlussjahrgängen oder Geburtsdaten der Teilnehmer. Deren IP-Adressen werden außerdem bei der Teilnahme nicht gespeichert. Um zudem die Identifizierung ehemaliger Nachhilfeschüler, die in ungewöhnlicheren Studienfächern ihren Abschluss gemacht haben aufgrund dieser Informationen zu verhindern werden Studienfächer nicht gesondert abgefragt, sondern lediglich verschiedene Studienfelder erfasst, bspw. „Naturwissenschaften“, „Rechts- und Wirtschaftswissenschaften“, „Sozial- und Erziehungswissenschaften“ und „Sprach- und Kulturwissenschaften“.²⁶

In diesem Beispiel versucht der Nachhilfeanbieter die Erfassung von Informationen zu vermeiden, die eine Identifizierung einzelner Umfrage-Teilnehmer ermöglichen, z. B. aufgrund ihres Namens, Geburtsdatums oder sogar ungewöhnlicher Studienfächer. Durch die Reduzierung der erfassten Menge an Daten auf das notwendige Minimum zur Auswertung der Umfrage ist die Wahrscheinlichkeit einer Re-Identifizierung der Teilnehmer verschwindend gering. Deshalb ist die Anonymisierung der Daten erfolgreich und die DSGVO findet keine Anwendung.

Vorteile der Anonymisierung

Die Anonymisierung bietet eine Reihe von Vorteilen für den Verantwortlichen/Auftragsverarbeiter. Unternehmen sammeln und speichern häufig große (manchmal sogar exzessive) Datenmengen, obwohl sie letztlich nur einen kleinen Teil der Datenmenge für ihre Verarbeitungstätigkeiten benötigen. Die *Nicht-Erfassung oder Löschung* der überschüssigen Daten kann dabei helfen, eine Anonymisierung der Daten herbeizuführen, um so die Anwendbarkeit der DSGVO zu verhindern. In Bezug auf die Verarbeitung rein anonymer Daten unterliegt der Verantwortliche/Auftragsverarbeiter nicht den verschiedenen Datenschutzverpflichtungen der Verordnung (siehe Kap. 3). Zusätzlich kann eine derartige *Datenminimierung* Zeit, Kosten und personelle Ressourcen einsparen. Unternehmen sollten das Inkrafttreten der DSGVO als Chance begreifen und den möglichen Einsatz von Anonymisierungstechniken in Betracht ziehen, damit die Anwendbarkeit der DSGVO und entsprechend das Risiko eines bußgeldbewährten Datenschutzverstößes minimiert werden kann.

Praxishinweise²⁷

Da sich der europäische Gesetzgeber bislang nicht zu den Standards für eine erfolgreiche Anonymisierung geäußert hat, ist zur Verbesserung der Datensicherheit eine Kombination von Randomisierungs- und Verallgemeinerungstechniken ratsam.

²⁶ Siehe auch Dammann, in: Simitis, BDSG, § 3 (2014), Rn. 201 ff.

²⁷ Siehe auch Art.-29-Datenschutzgruppe, WP 216 (2014), S. 6, 7, 12, 16, 23–25

Da der Anonymisierung stets ein *Risikofaktor* anhaftet, muss dieser bei der Bewertung verfügbarer Anonymisierungstechniken entsprechend der Schwere und Wahrscheinlichkeit des identifizierten Risikos Berücksichtigung finden. Als Konsequenz daraus ergibt sich, dass die optimale Anonymisierungslösung stets auf Einzelfallbasis zu bestimmen ist. Dies schließt eine *Bewertung des Verarbeitungskontextes* ein: „alle“ Mittel, die „vernünftigerweise“ für eine Re-Identifikation zur Verfügung stehen, müssen Berücksichtigung finden. Sobald die optimale Anonymisierungslösung gefunden ist, erfordert ihre Anwendung eine sorgfältige technische Implementierung, um die Widerstandsfähigkeit der technologischen Umsetzung zu erhöhen. Auch nach ihrer Anwendung bedarf die Anonymisierungstechnik einer *durchgehenden Überwachung*, um dem ihr inhärenten Risikopotenzial effektiv zu begegnen, vor allem was das Identifizierungsrisiko bzgl. nicht-anonymisierter Teile der Datenbank betrifft.

Pseudonymisierung

Pseudonymisierung ist in der Praxis ein gebräuchliches Mittel, um die Möglichkeit zur Identifikation betroffener Personen anhand ihrer Daten zu vermeiden. Es handelt sich um die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten *ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet* werden können, Art. 4 Nr. 5 DSGVO. Dies kann erreicht werden, indem der Name des Betroffenen oder andere Merkmale durch bestimmte Angaben ersetzt werden. Die zusätzlichen Informationen, die eine Identifizierung möglich machen würden, müssen *gesondert aufbewahrt* werden. Außerdem muss die Pseudonymisierung durch den Einsatz technischer und organisatorischer Mittel zusätzlich gesichert werden. Dies kann über eine *Verschlüsselung* der Daten erreicht werden, wobei der Schlüssel nur wenigen Personen mitgeteilt wird.

Es muss beachtet werden, dass, im Gegensatz zu anonymisierten Daten, pseudonymisierte Daten noch in den *Anwendungsbereich der DSGVO* fallen, da das Risiko einer Re-Identifikation höher ist als bei anonymisierten Daten. Nichtsdestotrotz handelt es sich bei der Pseudonymisierung um eine Möglichkeit für Verantwortliche und Auftragsverarbeiter, ihre Datenschutzverpflichtungen nach der DSGVO zu erfüllen und deren Einhaltung so auch nachzuweisen:²⁸

- Pseudonymisierung ist ein geeignetes Mittel zur Umsetzung des Prinzips des Datenschutzes durch Technikgestaltung (siehe Abschn. 3.7).
- Pseudonymisierung kann das Risikopotenzial der Verarbeitungstätigkeiten auf solche Weise verändern, dass der Verantwortliche von seiner Pflicht zur Meldung von Datenschutzverletzungen bzgl. der pseudonymisierten Daten entbunden wird (siehe Abschn. 3.8).
- Pseudonymisierung kann eine geeignete Schutzmaßnahme darstellen, um einen Wechsel des Verarbeitungszwecks zu rechtfertigen (siehe Abschn. 4.2.2.5).

²⁸ ErwGr. 28 DSGVO; Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), Rn. 27, siehe letztere auch für die nachfolgenden Ausführungen

- Erfolgreiche Pseudonymisierung kann zugunsten des Verantwortlichen in all jenen Fällen berücksichtigt werden, in denen seine Interessen gegen die der betroffenen Personen abzuwägen sind, z. B. in Fällen, bei denen die Datenverarbeitung auf die überwiegenden berechtigten Interessen des Verantwortlichen gestützt werden soll (siehe Abschn. 4.2.2.2).

Beispiel

Eine Unternehmensgruppe besteht u. a. aus den Unternehmen A und B. A sammelt personenbezogene Daten von den Kunden der Unternehmensgruppe, während B die personenbezogenen Daten erhält, um ein Profiling durchzuführen (Kundenpräferenzen, etc.). Bevor B die Daten erhält, werden sie jedoch pseudonymisiert, indem die persönlichen Kundeninformationen, wie Namen und Adressen, entfernt und durch Referenznummern ersetzt werden. Die Zuordnungsregel für die Referenznummern wird vom gemeinsamen Datenschutzbeauftragten der Unternehmensgruppe aufbewahrt, der angewiesen ist, die Zuordnungsregel gegenüber den Angestellten von B nicht offenzulegen.

In diesem Beispiel ist es B nicht möglich, die Daten den jeweiligen Kunden ohne Kenntnis der Zuordnungsregel zuzuordnen, wobei letztere B nicht bekannt ist. Die personenbezogenen Daten sind daher für B pseudonymisiert. Allerdings sind die Daten nicht anonymisiert und die DSGVO findet Anwendung, da ein gewisses Re-Identifikationsrisiko besteht. Es kann nicht mit hinreichender Sicherheit davon ausgegangen werden, dass B keine Kenntnis von der Zuordnungsregel oder von der Identität einzelner Kunden erlangt, z. B. durch andere Angestellte (von A) oder für den Fall, dass der Datenschutzbeauftragte seine Anweisungen verletzt.²⁹

Erfolgreiche Pseudonymisierung kann Datenschutz gewährleisten. Im Umkehrschluss bedeutet dies jedoch für den Fall, dass die angewandte Pseudonymisierungstechnik den Schutz der zusätzlichen Informationen nicht hinreichend gewährleisten kann, dass die Datenschutzverpflichtungen nach der DSGVO auf andere Weise oder durch zusätzliche technische und organisatorische Maßnahmen zu erfüllen sind.³⁰

2.1.3 Ausnahmen vom sachlichen Anwendungsbereich

Art. 2 Abs. 2 DSGVO sieht vier Ausnahmen vom sachlichen Anwendungsbereich der Verordnung vor. Unter anderem ist die Verordnung nicht in den Bereichen der Sicherheitspolitik (lit. b) oder der Strafverfolgung (lit. d) anwendbar. Aus wirtschaftlicher Sicht ist die wichtigste Ausnahme jedoch in lit. c geregelt, nach der die Verordnung keine Anwendung auf die „Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung *ausschließlich persönlicher oder*

²⁹ Beispiel aus Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), Rn. 30

³⁰ ErwGr. 26 DSGVO