

Tim Wybitul (Hrsg.)

EU-Datenschutz- Grundverordnung

Handbuch EU-Datenschutz-Grundverordnung

Schriftenreihe Kommunikation & Recht

Herausgegeben von

Professor Dr. Bernd Holznagel, LL.M., Münster

Professor Dr. Christian König, LL.M., Bonn

Professor Dr. Joachim Scherer, LL.M., Frankfurt am Main

Dr. Thomas Tschentscher, LL.M., Frankfurt am Main

Handbuch EU-Datenschutz- Grundverordnung

Herausgegeben von

Tim Wybitul

Rechtsanwalt, Frankfurt am Main

Mit Beiträgen von

Dr. Christoph Bausewein; Dr. Wolf-Tassilo Böhm;
Dr. Oliver Draf; Dr. Diana Ettig, LL.M.; Armin Fladung;
Dr. Henrik Hanßen; Dr. Stefan Krätschmer; Dr. Martin Pflüger;
Dr. Stephan Pötters, LL.M. (Cambridge); Dr. Nils Rauer, MJI;
Dr. Marcus Schreibauer; Dr. Stefan Schuppert, LL.M. (Harvard);
Paul Sigel; Jan Spittka; Jörg Steinhaus, M.A., LL.M.;
Dr. Lukas Ströbel; Dr. Christian Tinnefeld

Zitiervorschlag:

Bearbeiter, in: Wybitul, Handbuch DSGVO, 1. Aufl. 2017, Art. ..., Rn. ...

Wybitul, Handbuch DSGVO, 1. Aufl. 2017, Einl., Rn. ...

Bibliografische Information der Deutschen Nationalbibliothek

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

I S B N 978-3-8005-1623-0

dfv Mediengruppe

© 2017 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft,
Frankfurt am Main

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Kösel GmbH & Co. KG, 87452 Altusried-Krugzell

Printed in Germany

Vorwort

Die EU-Datenschutz-Grundverordnung (DSGVO) gilt ab dem 25.5.2018. Setzen Unternehmen die Vorgaben der DSGVO nicht hinreichend um, drohen hohe Bußgelder, Schadensersatzprozesse und weitere Nachteile. Das vorliegende Handbuch soll Unternehmen dabei helfen, sich auf die Anforderungen der DSGVO vorzubereiten.

Die Autoren sind Praktiker aus Unternehmen und Beratung und verfügen über teilweise langjährige Erfahrung im Datenschutzrecht und Datenschutz-Management. Das vorliegende Handbuch gibt Empfehlungen zur Auslegung und Umsetzung der Anforderungen der DSGVO. Der Schwerpunkt der Darstellung liegt dabei auf der praktischen Arbeit im Datenschutz. Weder soll das Handbuch eine wissenschaftliche Abhandlung noch eine an die Rechtswissenschaft gerichtete Kommentierung ersetzen, es ist vielmehr eine Arbeitshilfe für Projekte zur Umsetzung der DSGVO und zur Schaffung der hierfür erforderlichen Prozesse und Strukturen. Dementsprechend liegt der Schwerpunkt der Darstellung auf den für die Wirtschaft wichtigen Themen, andere Aspekte, wie etwa die Mechanismen zur Zusammenarbeit und der Abstimmung zwischen den Aufsichtsbehörden, werden nur am Rande angesprochen.

Auch das derzeit in Bundestag und Bundesrat verhandelte Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) wird in dem vorliegenden Buch nicht berücksichtigt. Zwar scheint sich immer klarer abzuzeichnen, dass das DSAnpUG-EU und das darin geregelte neue BDSG wohl noch in dieser Legislaturperiode verabschiedet werden. Allerdings hat der Bundesrat den vorgelegten Entwurf teilweise massiv kritisiert und viele Änderungen gefordert, vgl. BR-Drucks. 110/17 (Beschluss). Daher ist nach wie vor offen, welche Regelungen des Entwurfs die Parlamentarier verabschieden und in welcher Form. Zudem bewerten die Aufsichtsbehörden für den Datenschutz einige Regelungen als europarechtswidrig, etwa die geplante Einschränkung der Betroffenenrechte. Einige Behörden haben angekündigt, diese Regelungen selbst dann nicht anzuwenden, wenn der Gesetzgeber sie im Rahmen der beabsichtigten Neufassung des BDSG tatsächlich beschließen sollte. Auch vor diesem Hintergrund beschränkt sich das vorliegende Handbuch auf die Anforderungen der DSGVO.

Viele Vorschriften der DSGVO sind auslegungsbedürftig. Das vorliegende Handbuch gibt Vorschläge zur Anwendung dieser Vorschriften. Es bleibt abzuwarten, in welchen Fällen Gerichte und Behörden den hier vorgeschlagenen Auslegungsansätzen folgen werden und in welchen Fällen nicht. Ebenso sind

Vorwort

bei der ersten Auflage eines Handbuchs zu einem derart komplexen Gebilde wie der DSGVO Fehler und Ungenauigkeiten leider unabwendbar. Die Autoren, der Verlag und der Herausgeber würden sich daher sehr über entsprechende Hinweise und Verbesserungsvorschläge freuen.

Kronberg, im März 2017

Tim Wybitul

Bearbeiterverzeichnis

Bausewein, Dr. Christoph	Rechtsanwalt und Syndikusrechtsanwalt, Konzerndatenschutzbeauftragter mit internationalem Zuständigkeitsbereich bei einem US-amerikanischen Technologieunternehmen
Böhm, Dr. Wolf-Tassilo	Rechtsanwalt, Senior Associate – Hogan Lovells International LLP, Frankfurt am Main
Draf, Dr. Oliver	Rechtsanwalt (Syndikusrechtsanwalt), Leiter Datenschutz – Allianz Deutschland AG, München
Ettig, Dr. Diana, LL.M.	Rechtsanwältin – DAMM Rechtsanwälte, Frankfurt am Main
Fladung, Armin	Rechtsanwalt, Compliance-Officer (TÜV), Ressortleiter Arbeitsrecht und Compliance – CAD-Institut und Arbeitgeberverband Chemie Rheinland-Pfalz, Ludwigshafen
Hanßen, Dr. Henrik	Rechtsanwalt, Associate – Hogan Lovells International LLP, Hamburg
Krätschmer, Dr. Stefan	Rechtsanwalt (Syndikusrechtsanwalt), Data Privacy Officer, Europe – IBM, Ehningen
Pflüger, Dr. Martin	Rechtsanwalt, Counsel – Hogan Lovells International LLP, München
Pötters, Dr. Stephan, LL.M. (Cambridge)	Rechtsanwalt – Seitz Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB, Köln
Rauer, Dr. Nils, MJJ	Rechtsanwalt, Partner – Hogan Lovells International LLP, Frankfurt am Main
Schreibauer, Dr. Marcus	Rechtsanwalt, Partner, Fachanwalt für Informationstechnologierecht – Hogan Lovells International LLP, Düsseldorf

Bearbeiterverzeichnis

Schuppert, Dr. Stefan, LL.M. (Harvard)	Rechtsanwalt, Partner – Hogan Lovells International LLP, München
Sigel, Paul	Wissenschaftlicher Mitarbeiter, Hogan Lovells International LLP, Frankfurt am Main
Spittka, Jan	Rechtsanwalt, Senior Associate – DLA Piper UK LLP, Köln
Steinhaus, Jörg, M.A., LL.M.	Datenschutzbeauftragter – Fresenius SE & Co. KGaA, Bad Homburg
Ströbel, Dr. Lukas	Rechtsanwalt, Associate – Hogan Lovells International LLP, Frankfurt am Main
Tinnefeld, Dr. Christian	Rechtsanwalt, Counsel – Hogan Lovells International LLP, Hamburg
Wybitul, Tim	Rechtsanwalt, Fachanwalt für Arbeitsrecht, Partner – Hogan Lovells International LLP, Frankfurt am Main

Inhaltsverzeichnis

Vorwort.....	V
Bearbeiterverzeichnis.....	VII
Abkürzungsverzeichnis.....	XXI

Teil 1 **Einleitung**

I.	Ziele, Umsetzung und Anwendung der DSGVO.....	2
1.	Ziele der Verordnung.....	3
2.	Inkrafttreten der DSGVO.....	4
3.	Von der DSGVO verwendete Begriffe.....	5
4.	Anwendungsbereich der DSGVO.....	6
a)	Sachlicher Anwendungsbereich: Welche Datenverarbeitung- gen sind betroffen?.....	6
b)	Räumlicher Anwendungsbereich: Wo gilt die Verordnung? ..	8
II.	Überblick über die Vorschriften der DSGVO – Was steht wo?	9
1.	Allgemeine Bestimmungen (Kapitel 1, Art. 1 bis Art. 4 DSGVO)	10
2.	Grundsätze der Verordnung (Kapitel 2, Art. 5 bis Art. 11 DSGVO)	11
3.	Rechte der betroffenen Person (Kapitel 3, Art. 12 bis Art. 23 DSGVO)	12
4.	Verantwortlicher und Auftragsverarbeiter (Kapitel 4, Art. 24 bis Art. 43 DSGVO).....	13
5.	Übermittlung personenbezogener Daten in Drittländer (Kapitel 5, Art. 44 bis Art. 50 DSGVO).....	14
6.	Aufsichtsbehörden (Kapitel 6 und 7, Art. 51 bis 76 DSGVO) ...	15
7.	Rechtsbehelfe, Haftung, Sanktionen (Kapitel 8, Art. 77 bis Art. 84 DSGVO)	15
8.	Besondere Datenverarbeitungssituationen (Kapitel 9, Art. 85 bis Art. 91 DSGVO).....	16
9.	Delegierte Rechtsakte und Durchführungsrechtsakte (Kapitel 10, Art. 92 und 93 DSGVO).....	17
10.	Schlussbestimmungen (Kapitel 11, Art. 94 bis Art. 99 DSGVO)	17
III.	Grundsätze der DSGVO.....	18
1.	Bedeutung der Grundsätze der DSGVO für die Praxis	18

Inhaltsverzeichnis

2.	Die einzelnen Prinzipien der DSGVO	19
a)	Rechtmäßigkeit (Verbot mit Erlaubnisvorbehalt) (Art. 5 Abs. 1 lit. a) DSGVO)	20
b)	Treu und Glauben (Fairness) (Art. 5 Abs. 1 lit. a) DSGVO)	20
c)	Transparenz (Art. 5 Abs. 1 lit. a) DSGVO)	20
d)	Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO)	21
e)	Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO)	22
f)	Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO)	22
g)	Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO)	22
h)	Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO)	22
i)	Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)	23
IV.	Praktische Folgen – Wichtige Änderungen auf einen Blick	24
1.	Grundlagen der DSGVO	24
a)	Vorrang der DSGVO vor anderen Rechtsvorschriften der Mitgliedstaaten	25
b)	Globale Anwendung der DSGVO	25
c)	Erweiterte Haftung für Verantwortliche und Auftrags- verarbeiter	26
d)	Höhere Bußgelder	28
2.	Neue Pflichten für Unternehmen	30
a)	Erweiterte Dokumentations- und Nachweispflichten	30
b)	Risikobasierter Datenschutz	31
c)	Informationspflichten des Verantwortlichen bei Datenerhebung	32
d)	Datenschutz-Folgenabschätzung	38
e)	Striktere Löschpflichten und Recht auf Vergessenwerden	42
f)	Erhebliche Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen	43
g)	Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen	44
h)	Verzeichnis von Verarbeitungstätigkeiten	45
i)	Datensicherheit	48
j)	Zusätzliche Verantwortung für Datenschutzbeauftragte	50
3.	Betroffenenrechte (Art. 15 ff. DSGVO)	54
a)	Recht auf Auskunft (Art. 15 DSGVO)	54
b)	Recht auf Berichtigung (Art. 16 DSGVO)	57
c)	Pflicht zur Löschung von Daten (Art. 17 DSGVO)	58
d)	Recht auf Vergessenwerden (Art. 17 Abs. 2 DSGVO)	60
e)	Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	61
f)	Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	62
g)	Widerspruchsrecht	63

h) Automatisierte Entscheidung im Einzelfall (einschließlich Profiling)	64
4. Gemeinsam für Verarbeitungen Verantwortliche.	65
5. Auftragsverarbeitung.	67
6. Datenaustausch im Konzern	70
7. Übermittlung personenbezogener Daten in Drittländer	71
a) Voraussetzungen grenzüberschreitender Datenübermittlungen in Drittländer	71
b) Datenschutzrechtliche Folgen des „Brexits“	80
8. Aufsichtsbehörden.	82
9. Bewertung der Veränderungen durch die DSGVO – Folgen für Unternehmen	83
V. Erlaubnistatbestände der DSGVO	84
1. Überblick	84
a) Datenverarbeitungen nach Art. 6 DSGVO.	85
b) Datenverarbeitungen auf der Grundlage von Einwilligungen	85
c) Verarbeitung besonderer Kategorien personenbezogener Daten	85
d) Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten.	85
e) Besondere Verarbeitungssituationen	86
2. Erfüllung einer vertraglichen Verpflichtung (Art. 6 Abs. 1 lit. b) DSGVO).	86
a) Erfüllung einer vertraglichen Pflicht	86
b) Sonstige Anforderungen aus Art. 5 DSGVO	87
3. Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DSGVO)	88
a) Funktion von Art. 6 Abs. 1 lit. f) DSGVO	88
b) Interessenabwägung	88
4. Zweckänderungen (Art. 6 Abs. 4 DSGVO)	91
5. Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c) DSGVO).	94
a) Anforderungen an Rechtsvorschriften nach Art. 6 Abs. 3 DSGVO	94
6. Lebenswichtiges Interesse, öffentliches Interesse oder Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. d), e) DSGVO)	95
7. Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO).	95
a) Anforderungen an Einwilligungen	95
b) Koppelungsverbot bei Einwilligungen	97
c) Einwilligungen in der Praxis	97
8. Verarbeitung besonderer Kategorien personenbezogener Daten	99
a) Erlaubnis zur Verarbeitung besonderer Kategorien personenbezogener Daten	99

b) Erlaubnistatbestände zur Verarbeitung von Daten nach Art. 9 Abs. 2 DSGVO	99
9. Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO)	101
a) Anwendungsbereich von Art. 10 DSGVO	101
b) Sonderfall: Datenverarbeitung für Compliance-Zwecke	102
10. Besondere Verarbeitungssituationen – insbesondere Beschäftigtendatenschutz	103
a) Beschäftigtendatenschutz nach Art. 88 DSGVO	103
b) Regelung durch Rechtsvorschriften	104
c) Regelung durch Kollektivvereinbarungen	105
d) Folgen des Anwendungsvorrangs der Verordnung für Informationsrechte des Betriebsrats	106
VI. Projektplanung und Checkliste zur Umsetzung der DSGVO im Unternehmen	107
1. Überblick zur Implementierung der DSGVO	108
a) Projektteam	108
b) Festlegung von Projektzielen	108
c) Ressourcenplanung	109
d) Budgetplanung	109
e) Bestandsaufnahme bestehender Datenschutzstrukturen	110
f) Verarbeitungsverzeichnis	110
g) Rechtmäßigkeitsgrundlagen	110
h) Gap-Analyse	110
i) Lösungsoptionen	111
j) Einbindung Datenschutzbeauftragter	111
k) Risikoanalyse DSGVO	112
l) Datenschutzkommunikation	112
m) Datenschutzberatung	112
n) Betriebsrat	113
o) Betriebsvereinbarungen	113
p) Datenschutzbildung und -sensibilisierung	113
q) Datenschutz-Management-System	114
r) Auftragsverarbeitung	116
s) Gemeinsam Verantwortliche	117
t) Beschwerdemanagement	117
u) Überprüfung bestehender Verträge	117
v) Einwilligungsmanagement	117
2. Projektplanung der Umsetzung	118
a) Vorphase	118
b) Voruntersuchung	118
c) Umsetzungsphase	118

3.	Besondere Herausforderungen	120
a)	Organisation	120
b)	IT-Prozesse und Anwendungen	121
4.	Regelbetrieb	121
5.	Fazit und Ausblick	122
VII.	Gesetzentwurf zur Anpassung des BDSG	123
1.	Entstehungsgeschichte	123
2.	Die für die Praxis wichtigsten Änderungen	124
3.	Zusammenfassung und Ausblick	125
	Anhang: Mustersammlung	126
	Muster 1	
	Maßnahmen zur Umsetzung der DSGVO im Unternehmen	126
	Grobschema für einen Ablaufplan zur Umsetzung der DSGVO .	126
	Anlage: Priorisierung der Maßnahmen (Beispiel)	131
	Muster 2	
	Verarbeitungsverzeichnis für Unternehmen (Art. 30 Abs. 1 DSGVO)	132
	Kontaktdaten Verantwortlicher	133
	Verzeichnis der Verarbeitungstätigkeiten	134
	Beispiel für die Anlage zur Beschreibung einzelner Verarbeitungen	135
	Muster 3	
	Datenschutz-Folgenabschätzung für Unternehmen, Art. 35 DSGVO	139
	Muster 4	
	Anlage Auftragsverarbeitung zum Vertrag	151
	Anhang 1: Angaben zur Datenverarbeitung	164
	Anhang 2: Datenschutzbeauftragter, Weisungsberechtigte, Weisungsempfänger	165
	Anhang 3: Technische und organisatorische Maßnahmen zum Datenschutz	166
	Anhang 4: Auflistung der für den Auftragnehmer tätigen Subunternehmer	172
	Muster 5	
	Ablaufplan bei Datenschutzverletzungen in Unternehmen	173
	Anlage: Mitarbeiteranweisung für Datenschutzverletzungen . .	178

Teil 2
Abdruck und Kurzkomentierung der für
Unternehmen wichtigsten Vorschriften der DSGVO

KAPITEL I
Allgemeine Bestimmungen

Art. 1	Gegenstand und Ziele	182
Art. 2	Sachlicher Anwendungsbereich	187
Art. 3	Räumlicher Anwendungsbereich	193
Art. 4	Begriffsbestimmungen	200

KAPITEL II
Grundsätze

Art. 5	Grundsätze für die Verarbeitung personenbezogener Daten	225
Art. 6	Rechtmäßigkeit der Verarbeitung	237
Art. 7	Bedingungen für die Einwilligung	255
Art. 8	Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft	255
Art. 9	Verarbeitung besonderer Kategorien personenbezogener Daten	265
Art. 10	Verarbeitung von personenbezogenen Daten über strafrecht- liche Verurteilungen und Straftaten	282
Art. 11	Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist	287

KAPITEL III
Rechte der betroffenen Person

Abschnitt 1
Transparenz und Modalitäten

Art. 12	Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person	292
---------	---	-----

Abschnitt 2
Informationspflicht und Recht auf Auskunft
zu personenbezogenen Daten

Art. 13	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	294
---------	--	-----

Art. 14	Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden	296
Art. 15	Auskunftsrecht der betroffenen Person.	298

Abschnitt 3 Berichtigung und Löschung

Art. 16	Recht auf Berichtigung	318
Art. 17	Recht auf Löschung („Recht auf Vergessenwerden“).	322
Art. 18	Recht auf Einschränkung der Verarbeitung	341
Art. 19	Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung.	348
Art. 20	Recht auf Datenübertragbarkeit	352

Abschnitt 4 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Art. 21	Widerspruchsrecht	357
Art. 22	Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	358

Abschnitt 5 Beschränkungen

Art. 23	Beschränkungen	365
---------	--------------------------	-----

KAPITEL IV Verantwortlicher und Auftragsverarbeiter

Abschnitt 1 Allgemeine Pflichten

Art. 24	Verantwortung des für die Verarbeitung Verantwortlichen.	368
Art. 25	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	379
Art. 26	Gemeinsam für die Verarbeitung Verantwortliche	403

Inhaltsverzeichnis

Art. 27	Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern.	414
Art. 28	Auftragsverarbeiter	426
Art. 29	Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters	458
Art. 30	Verzeichnis von Verarbeitungstätigkeiten	463
Art. 31	Zusammenarbeit mit der Aufsichtsbehörde	481

Abschnitt 2 Sicherheit personenbezogener Daten

Art. 32	Sicherheit der Verarbeitung	488
Art. 33	Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde	499
Art. 34	Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	515

Abschnitt 3 Datenschutz-Folgenabschätzung und vorherige Konsultation

Art. 35	Datenschutz-Folgenabschätzung	524
Art. 36	Vorherige Konsultation	546

Abschnitt 4 Datenschutzbeauftragter

Vor Art. 37		554
Art. 37	Benennung eines Datenschutzbeauftragten	555
Art. 38	Stellung des Datenschutzbeauftragten	565
Art. 39	Aufgaben des Datenschutzbeauftragten	577

Abschnitt 5 Verhaltensregeln und Zertifizierung

Art. 40	Verhaltensregeln	586
Art. 41	Überwachung der genehmigten Verhaltensregeln	596
Art. 42	Zertifizierung	600
Art. 43	Zertifizierungsstellen	605

KAPITEL V
Übermittlung personenbezogener Daten an Drittländer
oder an internationale Organisation

Art. 44	Allgemeine Grundsätze der Datenübermittlung	611
Art. 45	Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses	616
Art. 46	Datenübermittlung vorbehaltlich geeigneter Garantien	629
Art. 47	Verbindliche interne Datenschutzvorschriften	640
Art. 48	Nach dem Unionsrecht nicht zulässige Übermittlungen oder Offenlegungen	652
Art. 49	Ausnahmen für bestimmte Fälle	656
Art. 50	Internationale Zusammenarbeit zum Schutz personenbezogener Daten	668

KAPITEL VI
Unabhängige Aufsichtsbehörden

Abschnitt 1
Unabhängigkeit

Art. 51	Aufsichtsbehörde	671
Art. 52	Unabhängigkeit	672
Art. 53	Allgemeine Bedingungen für die Mitglieder der Aufsichts- behörde	673
Art. 54	Errichtung der Aufsichtsbehörde	674

Abschnitt 2
Zuständigkeit, Aufgaben und Befugnisse

Art. 55	Zuständigkeit	675
Art. 56	Zuständigkeit der federführenden Aufsichtsbehörde	675
Art. 57	Aufgaben	676
Art. 58	Befugnisse	679
Art. 59	Tätigkeitsbericht	681

KAPITEL VII

Zusammenarbeit und Kohärenz

Abschnitt 1

Zusammenarbeit

Art. 60	Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden	682
Art. 61	Gegenseitige Amtshilfe.	684
Art. 62	Gemeinsame Maßnahmen der Aufsichtsbehörden	686

Abschnitt 2

Kohärenz

Art. 63	Kohärenzverfahren	687
Art. 64	Stellungnahme des Ausschusses	688
Art. 65	Streitbeilegung durch den Ausschuss	690
Art. 66	Dringlichkeitsverfahren	691
Art. 67	Informationsaustausch	692

Abschnitt 3

Europäischer Datenschutzausschuss

Art. 68	Europäischer Datenschutzausschuss	693
Art. 69	Unabhängigkeit	693
Art. 70	Aufgaben des Ausschusses	694
Art. 71	Berichterstattung	697
Art. 72	Verfahrensweise	697
Art. 73	Vorsitz	698
Art. 74	Aufgaben des Vorsitzes	698
Art. 75	Sekretariat	699
Art. 76	Vertraulichkeit	700

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

Art. 77	Recht auf Beschwerde bei einer Aufsichtsbehörde	701
Art. 78	Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde	701

Art. 79	Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	702
Art. 80	Vertretung von betroffenen Personen	703
Art. 81	Aussetzung des Verfahrens	704
Art. 82	Haftung und Recht auf Schadensersatz	705
Art. 83	Allgemeine Bedingungen für die Verhängung von Geldbußen .	721
Art. 84	Sanktionen	744

KAPITEL IX

Vorschriften für besondere Verarbeitungssituationen

Art. 85	Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit	748
Art. 86	Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten	754
Art. 87	Verarbeitung der nationalen Kennziffer	755
Art. 88	Datenverarbeitung im Beschäftigungskontext	757
Art. 89	Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken	769
Art. 90	Geheimhaltungspflichten	775
Art. 91	Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften	778

KAPITEL X

Delegierte Rechtsakte und Durchführungsrechtsakte

Art. 92	Ausübung der Befugnisübertragung	781
Art. 93	Ausschussverfahren	782

KAPITEL XI

Schlussbestimmungen

Art. 94	Aufhebung der Richtlinie 95/46/EG	785
Art. 95	Verhältnis zur Richtlinie 2002/58/EG	785
Art. 96	Verhältnis zu bereits geschlossenen Übereinkünften	785

Inhaltsverzeichnis

Art. 97	Berichte der Kommission	786
Art. 98	Überprüfung anderer Rechtsakte der Union zum Datenschutz. .	786
Art. 99	Inkrafttreten und Anwendung	787
	Literaturverzeichnis	789
	Sachregister.	793

Abkürzungsverzeichnis

A. A./a. A.	andere Ansicht
Abl.	Amtsblatt
Abs.	Absatz
ADV	Auftragsdatenverarbeitung
a. E.	am Ende
AEUV	Vertrag über die Arbeitsweise der europäischen Union
a. G.	auf Gegenseitigkeit
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
Anm.	Anmerkung
AO	Abgabenordnung
Art.	Artikel
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BayDSG	Bayerisches Datenschutzgesetz
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BB	Betriebsberater (Zeitschrift)
BCM	Business Continuity Management (englisch, = Betriebliches Kontinuitätsmanagement)
BCR	Binding Corporate Rule (englisch, = Verbindliche Unternehmensregel)
BDSG	Bundesdatenschutzgesetz
BEM	Betriebliches Eingliederungsmanagement
Berliner BfDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKM	Betriebliches Kontinuitätsmanagement
BKRG	Bundeskrebsregisterdatengesetz
BMI	Bundesministerium des Inneren
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drucks.	Bundestagsdrucksache
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands

Abkürzungsverzeichnis

BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
C2C	Controller-to-Controller (englisch, = Verantwortlicher zu Verantwortlichem)
C2P	Controller-to-Processor (englisch, = Verantwortlicher zu Verarbeiter)
CB	Compliance Berater (Zeitschrift)
CCZ	Corporate Compliance Zeitschrift
CERT	Computer Emergency Response Team (englisch, = Informationssicherheit-Krisenreaktionsteam)
CMS	Compliance Management System
CR	Computer und Recht (Zeitschrift)
DANA	Datenschutznachrichten (Zeitschrift)
DB	Der Betrieb (Zeitschrift)
d. h.	das heißt
DIN	Deutsches Institut für Normung
DJT	Deutscher Juristentag
DLP	data loss leakage (detection and) prevention (englisch, = Datenverlustprävention)
DMS	Datenschutz Management System
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DPA 1998	Data Protection Act 1998
DPMS	(data) privacy management system (englisch, = Datenschutz Management System)
Dr.	Doktor
DSB	Datenschutzbeauftragter
DSGVO	Datenschutzgrundverordnung
DSRITB	Deutsche Stiftung für Recht und Informatik Tagungsband
DSRL	Datenschutzrichtlinie (95/46/EG)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBI	Deutsches Verwaltungsblatt
DViA	Auftragsdatenverarbeitung
EDV	elektronische Datenverarbeitung
EFTA	Europäische Freihandelsassoziation
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EMPL-Ausschuss	Ausschuss für Beschäftigung und soziale Angelegenheiten des Europäischen Parlaments
EMRK	Europäische Menschenrechtskonvention
Engl.	Englisch
ENISA	Europäische Agentur für Netz- und Informationssicherheit

EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energie-wirtschaftsgesetz)
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuR	Europarecht (Zeitschrift)
EUR	Euro
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
evtl.	eventuell
EWK	Europäischer Wirtschaftsraum
f.	folgend
ff.	folgende
FISA	Foreign Intelligence Surveillance Act (englisch, = Gesetz zur Überwachung in der Auslandsaufklärung)
Fn.	Fußnote
FTC	Federal Trade Commission (englisch, = Bundeshandelskom-mission)
GDD	Gesellschaft für Datenschutz und Datensicherheit
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
HaagBewÜbK	Haager Beweisüberkommen
HessDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
HR	Human Resources
Hrsg.	Herausgeber
i. S. d.	im Sinne des/der
i. V. m.	in Verbindung mit
ICC	International Chambers of Commerce (englisch, = interna-tionale Handelskammer)
IDW	Institut der Wirtschaftsprüfer in Deutschland
IKT	Informations- und Kommunikationstechnologie
inkl.	inklusive
IP	Internetprotokoll
ISO	Internationale Organisation für Normierung
IT	Informationstechnik
ITRB	IT-Rechts-Berater (Zeitschrift)

Abkürzungsverzeichnis

IT-SiG	IT-Sicherheitsgesetz
K&R	Kommunikation & Recht (Zeitschrift)
KVP	Kontinuierlicher Verbesserungsprozess
LAG	Landesarbeitsgericht
LDI NRW	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LDSG Baden- Württemberg	Landesdatenschutzgesetz Baden-Württemberg
LFD Baden- Württemberg	Landesbeauftragter für den Datenschutz Baden-Württemberg
LG	Landgericht
LIBE-Ausschuss	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments
lit.	litera (lateinisch, = Buchstabe)
LLP	Limited Liability Partnership
LT-Drucks.	Landtagsdrucksache
Mio.	Million(en)
MMR	MultiMedia und Recht (Zeitschrift)
m. w. N.	mit weiteren Nachweisen
NIS-Richtlinie	Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über die Maßnahmen zur Gewähr- leistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
OECD	Organisation für wirtschaftliche Zusammenarbeit und Ent- wicklung
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PERT	Privacy Emergency Response Team (englisch, = Daten- schutz-Krisenreaktionsteam)
PC	Personal Computer
PIA	Privacy Impact Assessment (englisch, = Datenschutz-Fol- genabschätzung)
PKPI	Privacy Key Performance Indicators (englisch, = Daten- schutzleistungskennzahlen)
PKRI	Privacy Key Risk Indicators (englisch, = Datenschutzrisi- koindikatoren)
PM	Pressemitteilung

PRE	Privacy Risk Exposure (englisch, = Datenschutzgefährdungsmaßstab)
PS	Prüfungsstandard (z.B. des IDW)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RFID	Radio frequency identification
RL	Richtlinie
Rn.	Randnummer
ROI	Return of Investment (englisch, = Kapitalrendite)
ROPI	Return on (Privacy) Investments (englisch, = Rentabilität der Datenschutzinvestitionen)
ROSI	Return on Security Investments (englisch, = Rentabilität der Sicherheitsinvestitionen)
Rs.	Rechtssache
S.	Seite
SCC	EU Standard Contractual Clauses (englisch, = EU-Standardvertragsklauseln)
Schl.-Hl. LDSG	Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz)
SLA	Service Level Agreement (englisch, = Dienstgütevereinbarung)
sog.	sogenannt
StGB	Strafgesetzbuch
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
u. a.	unter anderem
u. Ä.	und Ähnliches
u. U.	unter Umständen
UAbs.	Unterabsatz
Urt.	Urteil
US	United States (of America) (englisch, = Vereinigte Staaten [von Amerika])
USA	United States of America (englisch, = Vereinigte Staaten von Amerika)
USV	unterbrechungsfreie Stromversorgung
v.	von/vom
VG	Verwaltungsgericht
vgl.	vergleiche
VIP	Very important persons (englisch, = sehr wichtige Personen)
WP	working papers

Abkürzungsverzeichnis

z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZD-Aktuell	Newsdienst. ZD aktuell

Teil 1

Einleitung

Die Datenschutz-Grundverordnung (DSGVO) gilt ab dem 25.5.2018.¹ Sie regelt die Verarbeitung personenbezogener Daten einheitlich für die gesamte Europäische Union. Die DSGVO stellt Unternehmen vor einige Herausforderungen und bringt einen erheblichen Umsetzungsaufwand mit sich. Das vorliegende Handbuch soll Hilfestellungen für die Anwendung des neuen Rechts geben. Es fasst bisherige Erfahrungen aus der Implementierung der Verordnung² bei einer Reihe von Wirtschaftsunternehmen zusammen. Die Autoren sind erfahrene Praktiker aus dem Bereich des Datenschutzes, die Unternehmen bei der Umsetzung der Anforderungen des neuen Datenschutzrechts unterstützen. Sie erläutern die für die Verarbeitung personenbezogener Daten in der Unternehmenspraxis relevanten Artikel der DSGVO in klarer und einfacher Sprache.

Zur besseren Verständlichkeit und Übersichtlichkeit enthält das vorliegende Buch auch einen umfassenden Einführungsteil, der die für Unternehmen wichtigsten Neuerungen in knapper und komprimierter Form zusammenfasst.³ Dabei werden viele in der DSGVO vorgesehene Prozesse und Strukturen durch Schaubilder, Praxistipps, Checklisten oder Ablaufpläne anschaulich beschrieben. Ein weiterer Abschnitt dieses Einleitungsteils beschreibt die erforderlichen Projektschritte zur Umsetzung der Vorgaben der DSGVO und fasst diese Planungsschritte in Form einer Checkliste zusammen.⁴ Abschließend findet der Leser auch einige Muster, die ihn bei der Anwendung der DSGVO im Unternehmen unterstützen sollen.⁵

Das vorliegende Handbuch erläutert die für die Datenschutzpraxis in der Wirtschaft wichtigen Vorschriften der DSGVO und gibt Hilfestellungen für die prak-

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, ABl. L 119/1.

2 Soweit in diesem Handbuch von der „Verordnung“ die Rede ist, bezieht sich dies ebenso wie die Abkürzung „DSGVO“ auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, ABl. L 119/1.

3 Der Einführungsteil beruht im Wesentlichen auf einer geringfügig aktualisierten und angepassten Fassung des Praxisleitfadens EU-Datenschutz-Grundverordnung im Unternehmen, 1. Aufl. 2016.

4 Siehe hierzu Rn. 387.

5 Siehe hierzu Mustersammlung Rn. 402 ff.

Teil 1 Einleitung

tische Umsetzung der Anforderungen des neuen Datenschutzrechts. Dieses richtet sich vor allem an den Praktiker im Unternehmen. Daher steht die praktische Einführung der DSGVO im Unternehmen im Vordergrund.

- 4 Der Schwerpunkt dieses Handbuchs liegt somit nicht auf einer umfassenden wissenschaftlichen Bewertung des kommenden EU-Datenschutzes, sondern auf der Umsetzung der DSGVO. Der Gesetzentwurf der Bundesregierung für ein deutsches Anpassungsgesetz zur DSGVO und dessen mögliche Auswirkungen für die Praxis werden in einem eigenen Abschnitt kurz bewertet.⁶

I. Ziele, Umsetzung und Anwendung der DSGVO

- 5 Am 4.5.2016 veröffentlichte die Europäische Union (EU) die Endfassung der seit 2012 verhandelten DSGVO.⁷ Sie gilt nach einer gut zweijährigen Übergangsfrist ab dem 25.5.2018 und hebt die Richtlinie 95/46/EG⁸ (Datenschutzrichtlinie) auf.⁹ Die DSGVO wirkt dann in der gesamten Europäischen Union unmittelbar und direkt. Anders als bei einer EU-Richtlinie ist eine Umsetzung in das nationale Recht der Mitgliedstaaten nicht mehr erforderlich. Dies soll zu einer erheblichen Vereinheitlichung beim Datenschutz in der EU führen und einheitliche Wirtschaftsbedingungen schaffen, die den Binnenmarkt stärken sollen.¹⁰
- 6 Für Unternehmen hat die Verordnung¹¹ gravierende Folgen: Neben Schadensersatzklagen drohen bei Fehlern Bußgelder von bis zu vier Prozent des globalen (Konzern-)Umsatzes. Beteiligte Manager, Datenschutzler und sonstige Entscheidungsträger müssen bei Verstößen mit Geldbußen von bis zu 20 Millionen Euro rechnen. Zudem sind die inhaltlichen Anforderungen beim neuen Datenschutz sehr hoch. Sie betreffen viele Unternehmensbereiche, etwa IT, Personal, Compliance, interne Revision und Vertrieb.

6 Siehe hierzu Rn. 392 ff.

7 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) im Amtsblatt der Europäischen Union, ABl. L 119/1.

8 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

9 Art. 94 Abs. 1 DSGVO.

10 Vgl. Erwägungsgrund 7.

11 Soweit in der vorliegenden Einführung die Begriffe „Verordnung“ oder „DSGVO“ in Bezug genommen werden, bezieht sich dies auf die deutsche Endfassung der EU-Datenschutz-Grundverordnung, abrufbar etwa unter <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

Dieser Teil der Einführung zeigt, welche Ziele der EU-Gesetzgeber mit der Einführung der DSGVO verfolgt. Es beschreibt zudem, für welche Anwendungsfälle das neue Datenschutzrecht gilt. Der Schwerpunkt liegt dabei auf der Frage, bei welchen Datenverarbeitungen Unternehmen¹² die Vorgaben der Verordnung beachten müssen. 7

1. Ziele der Verordnung

Die Verordnung soll das Datenschutzrecht EU-weit vereinheitlichen.¹³ Das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten soll in der gesamten Union gleichmäßig hoch und einheitlich sein.¹⁴ Die Anwendung einer einzigen EU-Verordnung zum Datenschutz soll es Unternehmen ermöglichen, die Datenverarbeitung in allen 28 Mitgliedstaaten gleich zu regeln. Diese Vereinheitlichung soll auch den Binnenmarkt in der Union stärken.¹⁵ 8

Allerdings enthält die Verordnung auch eine Reihe von sogenannten „Öffnungsklauseln“. Diese Vorschriften erlauben es den Mitgliedstaaten, in gewissen Umfang für einzelne Datenverarbeitungen oder Anforderungen nationale Spezialgesetze zu schaffen, etwa beim Beschäftigtendatenschutz gemäß Art. 88 DSGVO. Dabei legt Erwägungsgrund 155 fest, dass diese Öffnungsklausel es den Mitgliedstaaten vor allem erlaubt, Vorschriften über die Bedingungen vorzusehen, unter denen personenbezogene Daten im Beschäftigungsverhältnis auf Basis der Einwilligung¹⁶ eines Beschäftigten verarbeitet werden dürfen.¹⁷ 9

Solche Ausnahmenvorschriften müssen jedoch den grundsätzlichen Vorgaben der DSGVO entsprechen.¹⁸ Im Ergebnis beschränken die Öffnungsklauseln das Maß an EU-weiter Vereinheitlichung. Daher bleibt in vielen Bereichen abzuwarten, ob und in welcher Form die Mitgliedstaaten nationale Regelungen zum Beschäftigtendatenschutz erlassen werden – und welchen Spielraum der Europäische Gerichtshof (EuGH) ihnen hierfür letztlich zubilligen wird.¹⁹ Allerdings legt Erwägungsgrund 8 nahe, dass einzelstaatliche Regelungen nur in eingeschränktem Umfang möglich sind: „Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorge- 10

12 Vgl. zum Begriff des Unternehmens Art. 4 Nr. 18 DSGVO.

13 Vgl. Erwägungsgründe 10 ff.

14 Vgl. Erwägungsgrund 10.

15 Vgl. Erwägungsgründe 2 und 13.

16 Vgl. zum Begriff der Einwilligung Art. 4 Nr. 11 DSGVO.

17 Vgl. auch Kort, DB 2016, 711, 715.

18 Vgl. zum Regelungsrahmen bei Präzisierungen zum Beschäftigtendatenschutz etwa Art. 88 Abs. 2 DSGVO. Ausführlich hierzu auch Rn. 310 ff.

19 Vgl. Erwägungsgrund 8, der lediglich „Präzisierungen oder Einschränkungen [...] durch das Recht der Mitgliedstaaten“ erlaubt.