

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 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

IX

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 „Brexit“	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 Kurzkommentierung 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