

Inhaltsübersicht

Vorwort	5
I. DSGVO – Was ist das?	11
1. Was hat es mit der neuen Datenschutz-Grundverordnung auf sich?	12
2. Ein Hauptproblem der DSGVO	15
3. Für wen und was gilt die DSGVO?	16
4. Struktur der Datenschutz-Grundverordnung	17
II. Begriffe der DSGVO	23
1. „Personenbezogene Daten“	23
2. „Betroffene Person“	24
3. „Besondere Kategorien personenbezogener Daten“ gemäß Art. 9 DSGVO	25
4. „Verantwortlicher“	27
5. „Verarbeitung“	27
6. „Einwilligung“	28
7. „Dritter“	29
8. „Unternehmen“	29
9. „Empfänger“	29
10. „Verletzung des Schutzes personenbezogener Daten“	29
11. Weitere Definitionen	30
III. Die Grundsätze der DSGVO	33
1. Rechtmäßigkeit der Datenverarbeitung	33
2. Verarbeitung nach Treu und Glauben	35
3. Transparenz	35
4. Zweckbindung	38
5. Datenminimierung	40
6. Richtigkeit	41
7. Speicherbegrenzung	41
8. Integrität und Vertraulichkeit	42
9. Datenübermittlung in Drittstaaten	43
10. Rechenschaftsprinzip	45
IV. Projekt DSGVO-Umsetzung	47
1. Einbindung des Datenschutzbeauftragten	49
2. Projektteam benennen	52
3. Überblick verschaffen und Gap-Analyse	53

4.	Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) . . .	54
5.	Risiken ermitteln und abschätzen	60
6.	Einwilligungen prüfen	63
	a) Formular für Einwilligungen neu fassen	63
	b) Einwilligung eines Kindes	64
	c) Überprüfung bestehender Einwilligungen in Datenspeicherung und -verarbeitung	65
7.	Datenschutzfreundliche Grundeinstellungen	67
8.	Überprüfung von Verträgen mit Dienstleistern/Auftragsverarbeitung	68
V.	Zulässigkeit der Datenverarbeitung	71
1.	Einhaltung der Erlaubnistatbestände	71
	a) Einwilligung, Art. 6 Abs. 1 a	71
	b) Vertrag	73
	c) Gesetzliche Verpflichtung (Art. 6 Abs. 1 c DSGVO)	74
	d) Lebenswichtige Interessen	74
	e) Öffentliche Interessen	74
	f) Interessenabwägung, Art. 6 Abs. 1 f	75
2.	Abwägungen im Datenschutzrecht	76
3.	Dokumentation der Rechtmäßigkeit der Datenverarbeitung . . .	79
VI.	Betroffenenrechte beachten	81
1.	Informationspflichten umsetzen	81
	a) Informationspflichten bei Datenerhebung beim Betroffenen	82
	b) Informationspflichten bei Datenerhebung, die nicht bei der betroffenen Person stattfindet	86
2.	Das Auskunftsrecht (Art. 15 DSGVO)	87
3.	Recht auf Löschung („Vergessenwerden“) gemäß Art. 17 DSGVO	89
	a) Der EuGH begründet das Recht auf Vergessenwerden	90
	b) Recht auf Vergessenwerden in der DSGVO	91
	c) Vergessenwerden ist mehr als Löschen	92
4.	Recht auf Einschränkung der Verarbeitung	93
5.	Anspruch auf Berichtigung, Art. 16	94
6.	Recht auf Datenübertragbarkeit, Art. 20	95
7.	Widerspruchsrecht, Art. 21	96
8.	Art. 11 DSGVO: Verarbeitung ohne Identifizierung	97
VII.	Datenschutz-Management-System implementieren	99
1.	Erstellung und regelmäßige Überprüfung einer Datenschutzrichtlinie	100
2.	Rechtzeitige Feststellung relevanter Änderungen	101
3.	Wahrnehmung von Betroffenenrechten sicherstellen	102

4.	Feststellung und Reaktion auf Datenschutzverstöße/Datenpannen	103
5.	Kooperation mit der Behörde sicherstellen	103
6.	Datensicherheitsmanagement	104
7.	Das Standarddatenschutzmodell (SDM)	104
VIII.	Datensicherheit	107
1.	Sicherheitsstandards nutzen	110
2.	Einzelne Sicherheitsstandards	113
a)	ISO 27001	113
b)	VdS 3473	117
i.	Leitlinie zur Informationssicherheit	118
ii.	IT-Richtlinie für Mitarbeiter (und Kanzleiinhaber/Partner)	118
iii.	Richtlinie Mobilgeräte und tragbare Datenträger	120
iv.	Regelmäßige Schulungen, Vertraulichkeitserklärungen	121
v.	Richtlinie für IT-Dienstleister	122
vi.	Regelmäßige Informationen über neue Entwicklungen in der IT-Sicherheit	122
vii.	Rechtmanagement	122
viii.	Netzwerksicherung	123
ix.	Serverraum und Co.	123
x.	Datensicherung	123
xi.	Regelmäßig Sicherheitsmaßnahmen überprüfen	124
IX.	Sonderthemen	125
1.	Datenschutz-Folgenabschätzungen (DSFA)	125
a)	Fälle, in denen immer eine Datenschutz-Folgenabschätzung erfolgen muss	127
b)	Liegt eine „riskante Datenverarbeitung“ vor?	127
c)	Folgenabschätzung	128
d)	Einbeziehung betroffener Personen gemäß Art. 35 Abs. 9 DSGVO	128
e)	Konsultationsverfahren	129
f)	Bußgelder	129
2.	Was zu tun ist, wenn „es“ passiert – Data Breach (Art. 33, 34 DSGVO)	129
a)	Meldepflichten nach bisherigem Recht	130
b)	Neuregelung der DSGVO	130
c)	Anforderungen bei einer Datenpanne	131
3.	Kanzleiwerbung prüfen	135
a)	Überprüfung der Kanzleiwebsite	136
b)	Newsletter-Versand	138

4.	Datenschutz im Arbeitsverhältnis	138
a)	Arbeitnehmer als betroffene Personen	138
b)	Schulung und Sensibilisierung von Mitarbeitern	140
c)	Verpflichtung der Mitarbeiter auf das Datengeheimnis	141
X.	Sanktionen	143
1.	Bußgelder	143
2.	Verbandsklagerecht	146
3.	Schadensersatz	147
XI.	Zusammenfassung: 12 Punkte zur DSGVO	149
1.	Datenschutz als wichtiges Thema: Haftung und Bußgelder	149
2.	Prozesse analysieren	150
3.	Verzeichnis der Verarbeitungstätigkeiten	150
4.	Datenschutz-Folgenabschätzung	151
5.	Informationspflichten erfüllen	151
6.	Einwilligungen einholen	151
7.	Prüfen der Auftragsverarbeiter	151
8.	Betroffenenrechte umsetzen	151
9.	Bestandsdaten nicht vergessen	152
10.	Verantwortliche benennen	152
11.	Mitarbeiter schulen	152
12.	Datenschutzerklärung	152
	Checklisten	155
	Checkliste 1: Erforderliche Dokumente gemäß DSGVO	155
	Checkliste 2: Notfallplan	156
3.	Zum Weiterlesen	159