

Auf einen Blick

Über den Autor	8
Einführung	21
Teil I: Was sie ist	27
Kapitel 1: Ein Monster namens DSGVO	29
Kapitel 2: Personenbezogene Daten	47
Kapitel 3: Ziele des Datenschutzes	59
Kapitel 4: Die Protagonisten	79
Teil II: Was sie von Ihnen will	115
Kapitel 5: Die elf Gebote der DSGVO	117
Kapitel 6: Nicht erlaubt ist auch verboten	139
Kapitel 7: Zusammenarbeit von Unternehmen	161
Kapitel 8: Die Waffen der Betroffenen	199
Teil III: Wie Sie es am besten machen	237
Kapitel 9: Technisch-organisatorische Maßnahmen	239
Kapitel 10: Datenschutzmanagement	277
Kapitel 11: Spezialthemen	323
Kapitel 12: Sie als Betroffener	349
Teil IV: Der Top-Ten-Teil	367
Kapitel 13: Vorsicht Falle! Zehn Fallen für Datenschützer	369
Stichwortverzeichnis	379

Inhaltsverzeichnis

Über den Autor	8
Einführung	21
Über dieses Buch	21
Konventionen in diesem Buch	22
Was Sie nicht lesen müssen	23
Annahmen über Sie, den Leser	23
Wie dieses Buch aufgebaut ist	24
Teil I: Was sie ist	24
Teil II: Was sie will	24
Teil III: Wie Sie es am besten machen	25
Teil IV: Der Top-Ten-Teil	25
Symbole, die in diesem Buch verwendet werden	25
Wie es weitergeht	26
TEIL I	
WAS SIE IST	27
Kapitel 1	
Ein Monster namens DSGVO	29
Rechtliche Einordnung	30
Richtlinien	30
Verordnungen	31
Gründe für die Notwendigkeit einer Datenschutzreform	32
Uneinheitliche Umsetzung der europäischen Datenschutz-Richtlinie 95/46/EG	32
National unabhängige und eigenständige Datenschutzaufsichtsbehörden	33
Nationale Sonderregelungen – unterschiedliches Datenschutzniveau in den Mitgliedstaaten	33
Durchsetzbarkeit des europäischen Datenschutzstandards	34
Ziele der Reform	34
Mehr Kontrolle Betroffener über ihre Daten	34
Setzen globaler Standards für den Datenschutz	35
Einheitliche Datenschutzregeln für den digitalen Binnenmarkt	35
Inhalt	35
Erwägungsgründe	35
Verordnungstext	36
Unmittelbare Anwendbarkeit	36
Adressaten	38

12 Inhaltsverzeichnis

- Öffentliche Stellen 38
- Nicht öffentliche Stellen 39
- Haushaltsausnahme 39
- Sachlicher Anwendungsbereich der DSGVO 40
 - Verarbeitung personenbezogener Daten..... 40
 - Automatisierte Verarbeitung 41
 - Nicht automatisierte Verarbeitung 41
- Räumlicher Anwendungsbereich 41
 - Niederlassungsprinzip..... 41
 - Marktortprinzip 44
- Die Zähne des Monsters..... 46

Kapitel 2

Personenbezogene Daten 47

- Personenbezogene Daten 48
 - Einzelangaben..... 48
 - Natürliche Person 48
 - Persönliche Verhältnisse..... 49
 - Sachliche Verhältnisse..... 49
 - Bestimmte und bestimmbare Person..... 49
- Kategorisierung 50
 - Datenkategorien..... 51
 - Betroffenenkategorien 51
- Besondere Kategorien personenbezogener Daten 52
 - Angaben über die rassische und ethnische Herkunft 53
 - Angaben über politische Meinungen 54
 - Angaben über religiöse oder weltanschauliche Überzeugungen..... 54
 - Angaben zur Gewerkschaftszugehörigkeit..... 55
 - Genetische Informationen 55
 - Biometrische Informationen 56
 - Gesundheitsdaten 57
 - Informationen zum Sexualleben oder der sexuellen Orientierung 57
- Unangemessene Fragen..... 57
- Lösungsvorschläge 58

Kapitel 3

Ziele des Datenschutzes 59

- Bankgeheimnis..... 59
- Geschäftsgeheimnisse 60
- Geheimschutz 60
- Datensicherheit 60
 - Schutzziele..... 61
 - Gefahren 62
- Datenschutz 68
 - Schutzgut..... 68
 - Schutzziele des Datenschutzes 69

Kapitel 4	
Die Protagonisten	79
Die betroffene Person	79
Der Verantwortliche	80
Der Empfänger	81
Der Auftragsverarbeiter	82
Der Dritte	83
Die Aufsichtsbehörden	83
Wer sie sind	84
Was sie tun	86
Der Datenschutzbeauftragte	97
Stellung	97
Pflicht zur Benennung eines Datenschutzbeauftragten	100
Veröffentlichung der Kontaktdaten	104
Persönliche Voraussetzungen	105
Interner und externer Datenschutzbeauftragter	107
Highlander-Prinzip	110
Aufgaben	110
Haftung des Datenschutzbeauftragten	113
Der Datenschutzkoordinator	113

TEIL II **WAS SIE VON IHNEN WILL** **115**

Kapitel 5	
Die elf Gebote der DSGVO	117
Die 11 Gebote (Grundprinzipien) der DSGVO auf einen Blick	118
Grundsatz der Rechtmäßigkeit	119
Grundsatz von Treu und Glauben	119
Objektiver Erwartungshorizont	120
Verhältnismäßigkeitsgrundsatz	120
Transparenz	121
Zweckbindung	121
Datenminimierung	122
Richtigkeit	123
Aktualität	124
Speicherbegrenzung	125
Bemessung der Speicherdauer	126
Datenlöschung	129
Löschkonzept	130
Spezialthemen zur Speicherbegrenzung	133
Grundsatz der Integrität	136
Grundsatz der Vertraulichkeit	136
Vertraulichkeitsverpflichtung von Mitarbeitern	136
Beauftragung von Dienstleistern	137
Weitergabe von Daten	137
Grundsatz der Rechenschaftspflicht	138

Kapitel 6	
Nicht erlaubt ist auch verboten	139
Verbot mit Erlaubnisvorbehalt	140
Die einzelnen Erlaubnistatbestände	140
Verarbeitung zu vertraglichen oder vorvertraglichen Zwecken	141
Rechtliche Verpflichtung	143
Lebenswichtige Interessen	143
Berechtigtes Interesse	144
Zulässige Zweckänderung	148
Einwilligung	149
Auftragsverarbeitung, Art. 28	154
Besondere Kategorien personenbezogener Daten	154
Vorliegen einer qualifizierten Einwilligung	155
Arbeits- und sozialrechtliche Sondervorschriften	155
Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit	156
Sondervorschriften für Tendenzbetriebe	156
Offenkundig öffentlich gemachte Informationen	156
Durchsetzung von Rechtsansprüchen	157
Erhebliches öffentliches Interesse	157
Versorgung im Gesundheitsbereich	157
Öffentliche Gesundheitsdienste	158
Archivarische, wissenschaftliche und statistische Zwecke	158
Verarbeitung von personenbezogenen Daten über	
strafrechtliche Verurteilungen und Straftaten	159
Peinliche Fragen und blöde Antworten	159
Peinliche Fragen	159
Blöde Antworten	160
Kapitel 7	
Zusammenarbeit von Unternehmen	161
Lose Kooperationen	162
Gegenstand	162
Haftung	162
Vermittlungsgeschäfte	163
Gegenstand	163
Haftung	164
Auftragsverarbeitung	165
Gegenstand	165
Pflichten des Verantwortlichen	167
Rechte des Verantwortlichen	168
Pflichten des Auftragsverarbeiters	169
Vertragsgestaltung	177
Haftung	182
Typische Fallstricke	183
Vertragsökonomie	184
Datenübermittlung in Drittstaaten	186
Auftragsverarbeitung in Drittstaaten	187
Sonstige Formen der Datenübermittlung in Drittstaaten	191

Gemeinsame Verantwortliche	193
Gegenstand	194
Vertrag über gemeinsame Verantwortlichkeit	194
Haftung	196
Kleines Konzernprivileg	197

Kapitel 8

Die Waffen der Betroffenen..... 199

Was immer zu beachten ist	200
Präzise, transparent, verständlich	200
Klare und einfache Sprache	200
Formvorschriften	202
Identifizierung	203
Fristen	203
Unentgeltlichkeit	204
Missbrauch	204
Recht auf Information	205
Direkterhebung	205
Erhebung über Dritte	211
Nachträgliche Zweckänderung	215
Nachträgliche Informationspflichten	215
Sanktionen bei Verstößen gegen die Informationspflicht	215
Recht auf Auskunft	215
Inhalt	216
Form der Auskunft	218
Form der Antragstellung	218
Recht auf Berichtigung	218
Voraussetzungen	219
Inhalt	219
Form des Antrags	219
Zeitpunkt	220
Ausnahmen	220
Recht auf Löschung	220
Inhalt	220
Zeitpunkt	221
Ausnahmen	221
Recht auf Vergessenwerden	221
Voraussetzungen	222
Inhalt	222
Frist und Ausnahmen	222
Recht auf Einschränkung der Verarbeitung	222
Voraussetzungen	223
Inhalt	223
Zeitpunkt	223
Ausnahmen	224
Recht auf Datenübertragbarkeit	224

Voraussetzungen	224
Inhalt	224
Form	225
Zeitpunkt	226
Ausnahmen	226
Recht auf Widerspruch	226
Voraussetzungen	227
Inhalt	227
Hinweispflicht	229
Zeitpunkt	229
Ausnahmen	229
Ausschluss rein automatisierter Entscheidungen	230
Voraussetzungen	230
Inhalt	232
Form und Frist	232
Ausnahmen	232
Beschränkung von Betroffenenrechten	233
Recht auf Information bei Datenschutzverletzungen	233
Voraussetzungen	233
Folgen	234
Frist	234
Form	234
Ausnahmen	235

TEIL III

WIE SIE ES AM BESTEN MACHEN..... 237

Kapitel 9

Technisch-organisatorische Maßnahmen..... 239

Allgemeines	239
Vorgeschriebene Maßnahmen und Schutzziele	240
Pseudonymisierung	241
Verschlüsselung	242
Vertraulichkeit	242
Integrität	242
Verfügbarkeit	243
Belastbarkeit	243
Zugang	243
Intervenierbarkeit und Transparenz	244
Nichtverkettung	244
Datenminimierung	244
Regelmäßige Überprüfung, Bewertung und Evaluierung	244
Risikoanalyse	245
Verschiedene Ansätze	246
Schadensklassifizierung	248
Eintrittswahrscheinlichkeit	251
Risikoeinstufung	253
Festlegung von TOM	254

Technisch.....	254
Organisatorisch	255
Kriterien.....	256
Überblick über mögliche TOM	257
Datenschutzfolgenabschätzung	263
Wann?	264
Wer?	267
Wie?	267
Konsultation der Aufsichtsbehörde.....	272
Dokumentation der Datenschutzfolgenabschätzung.....	273
Verhaltensregeln	274
Zertifizierungen	275
Privacy by design and by default.....	275
Privacy by Design	275
Privacy by Default.....	276

Kapitel 10

Datenschutzmanagement..... 277

Integriertes Management-System.....	278
Datenschutzmanagement-System (PDCA).....	280
Projektplanung (Plan)	281
Umsetzung – Projektsteuerung und Abschluss (Do).....	301
Datenschutzaudit (Check).....	302
Maßnahmenfestlegung (Act)	308
Wichtige Dokumente.....	308
Verarbeitungsverzeichnis	309
Richtlinien	314
Arbeitsanweisungen	318
Kollektivvereinbarungen	318
Datenschutzinformationen.....	319
Datenschutzfolgenabschätzungen	319
Dokumentation von Datenschutzverletzungen.....	319
Dokumentation geltend gemachter Betroffenenrechte.....	320
Datenschutzprozesse	320
Datenschutzberichte	320
Auditberichte	320
Auftragsverarbeitungsverträge	320
Einwilligungen.....	320
Interne Sperrliste	321
Interessenabwägungen.....	321
Datenschutzhandbuch	322

Kapitel 11

Spezialthemen..... 323

Mitarbeiterdatenschutz	323
Rechtsgrundlagen	323
Bewerbungsverfahren.....	325

18 Inhaltsverzeichnis

- Personalakte 328
- Arbeitszeiterfassung 328
- Mitarbeiterfotos und -videos 329
- Privatnutzung von E-Mail, Geschäftstelefonen etc.. 329
- Informationspflichten 330
- Vertraulichkeitsverpflichtung 331
- Datenschutz in der Werbung 331
 - Rechtsgrundlagen 331
 - Empfehlungs- und Beipackwerbung für Angebote fremder Unternehmen 333
 - Kundenzufriedenheitsbefragungen 333
 - Daten aus Fremdbezug 334
 - Gewinnspiele 335
 - Bonussysteme 335
 - Hinweis auf das Widerspruchsrecht 336
- Datenschutzkonforme Website 336
 - Allgemeine Informationspflichten 336
 - Datenschutzinformationen – Datenschutzerklärung 337
 - Kontaktformulare 338
 - Nutzerkonten 338
 - Webshop 339
 - Newsletter 340
 - Blogs 340
 - Reichweitenmessung und Tracking 341
 - Cookies und Cookie-Banner 342
 - Social Plug-ins 343
 - Fanpages 344
- Messengerdienste 344
- Videoüberwachung 345
 - Rechtsgrundlagen 345
 - Hinweispflichten 347
 - Speicherdauer 348
 - Videoüberwachung in Echtzeit 348
 - Tonaufzeichnung 348

Kapitel 12

Sie als Betroffener 349

- Aufmerksamkeit. 350
- Anonymisierung im Internet 350
 - Betriebssystem 350
 - Browser 351
 - Virtual Private Network (VPN). 353
 - Vernichtung von Datenspuren 354
 - Gesichtserkennung 354
 - Device Fingerprinting. 354
- Verschlüsselung 355

Verschlüsselung des E-Mail-Verkehrs	355
Dateiverschlüsselung	357
Datenträgerverschlüsselung	357
Umgang mit Sprachassistenten	358
Tracking	359
Soziale Netzwerke	359
Arten von Daten	359
Privacy-Einstellungen	360
Allgemeine Geschäftsbedingungen	362
Betriebssystem	363
Cloud	364
Patches und Updates	364
Virens Scanner	364
Soziales Engagement	365
Betroffenenrechte	365

TEIL IV

DER TOP-TEN-TEIL	367
-------------------------------	------------

Kapitel 13

Vorsicht Falle! Zehn Fallen für Datenschützer	369
--	------------

Die Informationsfalle	369
Die Verarbeitungsfalle	370
Der Fisch stinkt vom Kopf her	371
Der Alibibeauftragte	371
Die Keinwilligung	372
Die Löschfalle	373
Aus dem Auge, aus dem Sinn	373
Die Meldefalle	374
Die Sicherheitsfalle	374
Die Beweisfalle	375

Stichwortverzeichnis	379
-----------------------------------	------------