

Inhalt

Vorwort	13
---------------	----

Teil I Einleitung	15
--------------------------	-----------

1 Einführung in die Datenschutz-Grundverordnung (DS-GVO)	17
1.1 Die Ausgangslage	17
1.2 Neuregelungen des Datenschutzes durch die DS-GVO	17
1.3 Fazit	30
2 Häufig gestellte Fragen und Irrtümer zur DS-GVO	31
2.1 „Die Datenschutz-Grundverordnung gilt nicht für kleine Unternehmen.“	31
2.2 „Vereine sind von der DS-GVO nicht betroffen.“	31
2.3 „Der deutsche Gesetzgeber wird für Ausnahmen sorgen.“	32
2.4 „Mit der DS-GVO ändert sich nichts.“	32
2.5 „Die Einhaltung kontrolliert doch keiner.“	32
2.6 „Wir verarbeiten keine personenbezogenen Daten.“	33
3 Warum Datenschutzverstöße kein Kavaliersdelikt (mehr) sind	35
3.1 Einleitung	35
3.2 Die Datenschutz-Grundverordnung	35
3.3 Was sich ändern wird	36
3.4 Rechtsgrundlagen: Wann dürfen Daten verarbeitet werden?	37
3.5 Betroffenenrechte: mehr Transparenz	39
3.6 Dokumentationspflichten	40
3.7 IT-Sicherheit	40
3.8 Neuerungen im Outsourcing	42
3.9 Haftung & Bußgelder	42
3.10 Datenschutzaufsicht	43
3.11 Paradigmenwechsel: Beweise die Unschuld	43
3.12 Fazit: erste Schritte zur Umsetzung	44
4 Datenschutz: Recht = DS-GVO + BDSG-neu – Änderungen für Unternehmen	45
4.1 Was ändert sich für Unternehmen?	47
4.2 Videoüberwachung öffentlich zugänglicher Räume	47
4.3 Pflicht zur Bestellung eines Datenschutzbeauftragten (§ 38 BDSG-neu)	48

4.4	Zusätzliche Erlaubnistatbestände zur Verarbeitung besonderer personenbezogener Daten (§§ 22, 24 BDSG-neu).....	49
4.5	Beschäftigtendatenschutz (§ 26 BDSG-neu)	49
4.6	Einschränkung des Auskunftsrechts (§ 34 BDSG-neu)	49
4.7	Fazit	50
5	Die zweite Stufe der Anpassung des Datenschutzrechts des Bundes an die EU-Datenschutz-Grundverordnung	51
5.1	Zentrale Aspekte der Anpassung des bereichsspezifischen Bundesrechts an die DS-GVO	51
5.2	Fazit und Ausblick	54
6	Wer ist datenschutzrechtlich „Verantwortlicher“ im Unternehmen?	57
6.1	Die bisherige Rechtslage	57
6.2	Die Rechtslage nach der DS-GVO	59
6.3	Fazit	67
7	Neue Aufgaben für (HR-)Fach- und Führungskräfte	69
7.1	Erweiterung des Aufgabenspektrums	69
7.2	Prozessanforderungen	70
7.3	Einkauf von Produkten und Dienstleistungen.....	72
7.4	Zusammenarbeit mit dem Betriebsrat	73
7.5	Fazit	73
8	Assessment-Tool zur DS-GVO-Readiness.....	75
9	Merkblatt Projektorganisation: Einführung der Datenschutz-Grundverordnung im Unternehmen.....	79
9.1	Hintergrundwissen: Projektorganisation	79
9.2	Phase: Awareness schaffen	80
9.3	Phase: Projekt strukturieren	82
9.4	Phase: Projekt planen	83
9.5	Phase: Projekt beginnt	85
9.6	Argumentationshilfen.....	85
Teil II Von der Rechenschaftspflicht zur Dokumentation		87
10	Dokumentationspflichten in der DS-GVO	89
10.1	Einleitung.....	89
10.2	Anforderungen an ein Dokumentationssystem	90
10.3	Inhalte der Dokumentation	92
10.4	Phase Planung.....	93
10.5	Zwecke und Rechtsgrundlagen.....	93

10.6	Interessenabwägung	93
10.7	Sicherheitskonzept	93
10.8	Beschreibung der Unternehmensprozesse	94
10.9	Phase Umsetzung	96
10.10	Phase Kontrolle	97
10.11	Phase Mängelbeseitigung	98
10.12	Das Verzeichnis von Verarbeitungstätigkeiten	98
10.13	Fazit	99
11	Das Schriftformerfordernis der Einwilligung nach § 4a BDSG im Pendelblick zu Art. 7 DS-GVO	101
11.1	Die Schriftlichkeit der Einwilligung zwischen BDSG und DS-GVO	101
11.2	Sinn und Zweck gesetzlicher Formerfordernisse	102
11.3	Die Rechtslage nach § 4a BDSG	103
11.4	Eigenständiger Schriftlichkeitsbegriff des BDSG	106
11.5	Das künftige Recht der DS-GVO: Art. 7 DS-GVO	111
11.6	Von der Schriftlichkeit zur Nachweispflicht.....	113
Teil III Die Arbeit des Datenschutzbeauftragten		115
12	Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben	117
12.1	Bestellung eines Datenschutzbeauftragten	117
12.2	Rechtsstellung des Datenschutzbeauftragten	122
12.3	Aufgaben des Datenschutzbeauftragten	125
12.4	Wegfall der Ermächtigungen zum Erlass delegierter Rechtsakte ...	129
12.5	Fazit	130
13	Die grundrechtskonforme Ausgestaltung der Datenschutz- Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung	131
13.1	Eine grundrechtskonforme Datenschutz-Folgenabschätzung.....	132
13.2	Übergang in die neue Welt der DS-GVO	146
13.3	Fazit	147
Teil IV Spezialgebiete: Werbung und Gesundheitswesen		149
14	Datenverarbeitung zu Werbezwecken nach der Datenschutz- Grundverordnung.....	151
14.1	Ausgangslage und Grundbedingungen der Rechtsanwendung unter der DS-GVO	152

14.2	Grundprinzipien des werbewirtschaftlichen Datenschutzes nach DS-GVO	156
14.3	Die materiellen Regelungen des werbewirtschaftlichen Datenschutzes nach der DS-GVO	157
14.4	Zwischenfazit.....	168
14.5	Datenverarbeitung zu Vertragszwecken oder für die Durchführung vorvertraglicher Maßnahmen	169
14.6	Datenverarbeitung aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten unter Abwägung mit den Interessen der betroffenen Person.....	171
14.7	Informationspflichten nach der DS-GVO	178
14.8	Werbewiderspruch	182
14.9	Szenarien werbewirtschaftlicher Datenverarbeitung unter der DS-GVO	184
14.10	Fazit	191
15	DS-GVO – Was ändert sich im Gesundheitswesen?	193
15.1	Begriffsbestimmungen.....	194
15.2	Rechtsgrundlagen für die Verarbeitung.....	195
15.3	Betroffenenrechte	197
15.4	Berufsgeheimnisträger	199
15.5	Vorgaben für das Unternehmen „Krankenhaus“ bzw. die „ambulante Versorgung“.....	200
15.6	Forschung	207
15.7	Sanktionen/Strafregelungen	210
15.8	Fazit	211
16	Zulässigkeit der Tätigkeit von Auskunfteien nach der DS-GVO	213
16.1	Rechtslage unter dem BDSG	213
16.2	Rechtslage unter der DS-GVO	214
16.3	Fazit	219
Teil V Betroffenrechte		221
17	Das System der Betroffenenrechte nach DS-GVO	223
17.1	Überblick	223
17.2	Betroffenenrechte nach Zielen	224
17.3	Zusammenfassung und Ausblick	239
18	Warum die neuen Betroffenenrechte im Datenschutz zur Falle werden können	241
18.1	Einleitung.....	241
18.2	Das Recht auf Datenübertragbarkeit in der Praxis.....	242

18.3	Verhinderung automatischer Entscheidungen	243
18.4	Fazit	243
19	Wie sag ich's nur? – Informationspflichten	245
19.1	Einleitung.....	245
19.2	Direkte und indirekte Erhebung.....	246
19.3	Zeitpunkt.....	247
19.4	Direkterhebung.....	247
19.5	Indirekte Erhebung	248
19.6	Form und Sprache.....	249
19.7	Inhalt	250
19.8	Ausnahmen	254
19.9	Informationspflichten bei neuen Zwecken.....	254
19.10	Notwendige Vorarbeiten.....	255
19.11	Folgen bei einem Verstoß	256
19.12	Fazit	256
Teil VI Auswirkungen auf die Personalwirtschaft		257
20	Was bleibt und was ist neu? Die EU-DS-GVO und der Beschäftigtendatenschutz.....	259
20.1	Die Ausgangslage	259
20.2	Nationale Beschäftigtendatenschutzregelungen	260
20.3	Neuregelungen der DS-GVO für den Beschäftigtendatenschutz	263
20.4	Fazit	276
21	Maßgeschneiderte Lösungen durch Kollektivvereinbarung? – Möglichkeiten und Risiken des Art. 88 Abs. 1 DS-GVO.....	277
21.1	Verhältnis von DS-GVO, BetrVG und TVG	277
21.2	Erste Schranke: Art. 88 Abs. 1 DS-GVO.....	278
21.3	Zweite Schranke: Nationales Recht (insb. BetrVG)	289
21.4	Was geschieht am 25.05.2018?.....	290
21.5	Risiken und Nebenwirkungen: Verstoß gegen die Schranken, Sanktionen	291
21.6	Fazit	292
22	Die Verarbeitung von Beschäftigtendaten im Rahmen betriebsverfassungsrechtlicher Aufgaben nach § 26 Abs. 1 S. 1 BDSG-n.F.....	293
22.1	Das neue BDSG auf der Zielgeraden.....	293
22.2	Wesentliche Regelungen des neuen § 26 BDSG-n.F.	295
22.3	Öffnungsklauseln der DS-GVO mit Relevanz für den Beschäftigtendatenschutz	296

22.4	Der Geltungsbereich des § 26 BDSG-n.F.	297
22.5	Datenverarbeitung des Arbeitgebers mit der Zweckbestimmung des § 26 Abs. 1 S. 1 Zulässigkeitsalternative 2 BDSG-n.F.	298
22.6	Datenverarbeitungen der Mitarbeitervertretung	302
22.7	Fazit	303
23	Beschäftigtendatenschutz: Zwischen wirtschaftlicher Abhängigkeit und informationeller Selbstbestimmung	305
23.1	Der Weg vom Volkszählungsurteil bis zur verfassungskonformen gesetzlichen Regelung	305
23.2	Die Welt des Beschäftigtendatenschutzes aus Sicht des LfDI BW	316
23.3	Das Ziel unserer Arbeit.....	338
24	Personalrecruiting (bald) ein risikoreiches Geschäft? Auswirkungen der DS-GVO im Bereich des Personalrecruitings	339
24.1	Zwei Jahre bis zum Vollzug – eine knappe Zeitspanne	339
24.2	Insolvenz durch Recruiting?	340
24.3	Informationspflichten im Bewerbungsprozess	340
24.4	Informationspflichten bei neuen Zwecken	345
24.5	Sicherheitsüberprüfungen und polizeiliche Führungszeugnisse	345
24.6	Automatisierte Entscheidungen und Profiling	346
24.7	Neue Rechte für Bewerber („Betroffenenrechte“)	346
24.8	Fazit	351
25	E-Learning in der Cloud – der Datenschutzcheck	353
25.1	Glossar	354
26	Gehaltsbenchmarks unterstützen – zulässig?	357
26.1	Einleitung.....	357
26.2	Personenbezug der übermittelten Daten.....	358
26.3	Rechtsgrundlagen für eine Übermittlung.....	358
26.4	Fazit	360
27	Pre-Employment-Screening – Eine rechtliche Herausforderung?	361
27.1	Einleitung.....	361
27.2	Rechtmäßigkeit des Pre-Employment-Screenings.....	362
27.3	Einwilligung	362
27.4	Informationspflichten	363
27.5	Einsatz von Dienstleistern	363
27.6	Fazit	364

Teil VII Auswirkungen auf die IT-Administration und IT-Sicherheit 365

28 Mehr gesetzliche Pflichten für IT-Verantwortliche – Auswirkungen auf die IT-Sicherheitsorganisation/das IT-Sicherheitsmanagement.....	367
28.1 Gesetzliche Vorgaben zur Sicherheitsorganisation.....	367
28.2 Sicherheitskonzeption	368
28.3 Wirksamkeitstest	370
28.4 Melde- und Dokumentationspflichten bei Sicherheitsvorfällen.....	370
28.5 Dokumentation von Sicherheitsvorfällen	371
28.6 Meldepflicht als Auftragnehmer.....	372
28.7 Meldepflicht gegenüber der Datenschutzaufsichtsbehörde	372
28.8 Information betroffener Personen.....	374
28.9 Gesetzliche Erlaubnis zur Datenverarbeitung	376
28.10 Informationspflichten über Datenverarbeitung	377
28.11 Gesetzliche Einkaufshilfe	378
28.12 Gesetzliche Konfigurationshilfe	379
28.13 Zertifizierung und Standards	379
28.14 Erste Schritte zur Umsetzung.....	380
28.15 Fazit	381
29 Neue Dokumentationspflichten in der IT	383
29.1 Einleitung.....	383
29.2 Anforderungen an eine Dokumentation.....	384
29.3 Inhalte der Dokumentation	385
29.4 Phase Planung.....	386
29.5 Sicherheitskonzept	386
29.6 Beschreibung der Unternehmensprozesse	386
29.7 Phase Umsetzung	388
29.8 Phase Kontrolle	389
29.9 Phase Mängelbeseitigung	390
29.10 Fazit	390
30 Am Anfang steht das Sicherheitskonzept	391
30.1 Einleitung.....	391
30.2 Neue Datenschutzanforderungen an ein Sicherheitskonzept – in vier Schritten zum Sicherheitskonzept	392
30.3 Diese Prozesse dürfen nicht fehlen.....	397
30.4 Neue Pflicht: Wirksamkeitstest.....	397
30.5 Fazit	398

31 Biometrische Zutrittskontrollen: ein Auslaufmodell?	399
31.1 Einleitung.....	399
31.2 Zulässiger Einsatz	400
31.3 Gestaltung des Zutrittskontrollsystems	403
31.4 Sicherheit	404
31.5 Informationspflichten	405
31.6 Fazit	406
32 Der übersehene Paragraph und die DS-GVO	407
32.1 Ersetzt die DS-GVO § 13 Abs. 7 TMG?	408
Teil VIII Auftragsdatenverarbeitung und Softwareanbieter	411
33 ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland	413
33.1 Zur Auftragsverarbeitung.....	413
33.2 Anforderungen an den Auftragnehmer.....	420
33.3 Unterauftragnehmer	429
33.4 Wartung/Fernwartung (§ 11 Abs. 5 BDSG).....	432
33.5 Auftragsdatenverarbeitung in Drittländern.....	432
33.6 Funktionsübertragung	433
33.7 Aufsichtsbehörden.....	436
33.8 Umsetzung von Standards	437
33.9 Zertifizierung	438
33.10 Fazit	438
34 (Fehlende) Privilegierung der Auftragsverarbeitung unter der Datenschutz-Grundverordnung?	441
34.1 Einleitung.....	441
34.2 Privilegierungswirkung der Auftragsdatenverarbeitung nach Datenschutzrichtlinie und BDSG	442
34.3 Datenweitergabe vom Auftraggeber an den Auftragnehmer nach der Datenschutz-Grundverordnung	443
34.4 Fazit	451
35 Datenschutz-Compliance bei der Auswahl von Dienstleistern	453
35.1 Einleitung.....	453
35.2 Gesetzliche Mindestinhalte des Vertrags	454
35.3 Formerfordernisse des Vertrags.....	456
35.4 Beauftragung von Unterauftragnehmern.....	456
35.5 Garantien zur Einhaltung von geeigneten technischen und organisatorischen Maßnahmen.....	457

35.6	Ort der Datenverarbeitung.....	458
35.7	Fazit	459
36	DS-GVO: Schicksalhafte Herausforderung für Softwareanbieter?	461
36.1	Einleitung.....	461
36.2	Steckbrief der gesetzlichen Anforderungen	461
36.3	HCM: Vorteile integrierter Produkte	466
36.4	Besonderheiten Cloud.....	466
36.5	Zertifizierungen als Compliance-Nachweise	468
36.6	Fazit	468
37	Datenschutz „by Design“ und „by Default“ nach der neuen europäischen Datenschutz-Grundverordnung.....	469
37.1	Datenschutz „by Design“ – Art. 25 Abs. 1 DS-GVO	470
37.2	Datenschutz „by Default“ – Art. 25 Abs. 2 DS-GVO.....	473
37.3	Rolle der Zertifizierung – Art. 25 Abs. 3 DS-GVO	475
37.4	Hinweise für den Anwender	476
37.5	Fazit	478
38	Technische Herausforderungen in der DS-GVO – Im Spannungsfeld zwischen Prüfungen und Sanktionen	479
38.1	Ausgangslage: DS-GVO und rechtliche Bewertungen in der Informationstechnik	479
38.2	Rahmenbedingungen und unterschiedliche Lesarten aus der Perspektive der IT-Entwicklung.....	481
38.3	Die Aufsichtsbehörde	491
38.4	Die Prüfung	496
38.5	Zusammenfassung.....	497
Teil IX Compliance-Kosten vs. Nutzen		499
39	Wann kostet ein Personenbezug zu viel?	501
39.1	Einleitung.....	501
39.2	Welche Daten dürfen verarbeitet werden?.....	502
39.3	Compliance-Kosten vs. Nutzen	502
39.4	Fazit	504
Teil X Umgang mit Altverhältnissen		505
40	Altverhältnisse unter DS-GVO und neuem BDSG – Anwendung des neuen Datenschutzrechts auf bereits laufende Datenverarbeitungen?	507
40.1	Überblick	507

40.2	Einwilligungen	507
40.3	Verträge zur Auftragsverarbeitung	509
40.4	Betriebsvereinbarungen	511
40.5	Instrumente des Drittstaatstransfers	512
40.6	Datenschutzbeauftragte	513
40.7	Transparenzregeln bei der Datenerhebung	513
40.8	Datenschutz-Folgenabschätzungen.....	514
40.9	Verpflichtungen auf das Datengeheimnis.....	516
40.10	Fazit	516
41	Altpannen und Alt-Ordnungswidrigkeiten unter der DS-GVO	517
41.1	Meldung vorangegangener Datenpannen.....	517
41.2	Bußgelder für Altverstöße	518
41.3	Zusammenfassung.....	520
Index	521
Mitwirkende an diesem Buch	525