Inhaltsverzeichnis

Seite

Vorwort V
Bearbeiterverzeichnis XV
Abkürzungsverzeichnis XVII
Literaturverzeichnis XXXI

A. Organisationsstruktur Datenschutz

I. Rechenschaftspflicht (Art. 5, 24 DS-GVO) 1

II. Datenschutz-Compliance 12
1. Vorstandspflichten – die Lücke zwischen Datenschutzbeauftragtem und Datenschutz-Compliance 12
2. Pflichten und Haftung von Vorständen bzw. Geschäftsleitung sowie von Aufsichtsräten 15
3. Anforderungen an ein Compliance-Management-System nach IDW PS 980 und DS-GVO-Prüfung nach IDW PH 9.860.1 18

III. Datenschutzorganisation im Unternehmen 23
1. Organisatorischer und strategischer Aufbau 23
2. Pflichtübung, Kür oder Privacy-Manager: vom Datenschutzbeauftragten zu Datenschutz-Compliance 30
3. Dienstleister oder Kontrolleur: die zwei Gesichter von Datenschutzabteilungen 35
4. Von der Auftragsverarbeitung bis zur Verbandsarbeit: Zuständigkeitsbereiche im Einzelnen 39
5. Risikoverständnis und Reifegrad einer Datenschutzorganisation 42
6. Umgang mit Anfragen und Audits der Aufsichtsbehörden 45
7. Arbeitsweise am Beispiel Datenschutz-Folgenabschätzung: Dienst nach Vorschrift oder Teamarbeit 49

IV. Code of Conduct und Selbstverpflichtung zum Datenschutz 57
1. Datenschutz im Code of Conduct 57
2. Übersicht zu Hinweisgebersystemen (Whistleblower-Hotlines) 60
3. Hinweisgebersystem (Whistleblower-Hotline) im Code of Conduct ... 62
4. Datenschutzerklärung für ein elektronisches Hinweisgeberportal 64
5. Richtlinie zum Einsatz eines Hinweisgebersystems 65
6. Internal Investigations: Unternehmenspflicht vs. Datenschutz 74

B. Der Datenschutzbeauftragte

I. Benennung und Abberufung des Datenschutzbeauftragten 77
1. Benennung als Datenschutzbeauftragter 77
2. Abberufung durch den Arbeitgeber 96

II. Verträge mit externen Datenschutzbeauftragten 102
1. Dienstvertrag mit einem externen Datenschutzbeauftragten 102
2. Beratungsvertrag mit einem Dienstleistungsunternehmen 121
3. Aufhebungsvertrag der Parteien 132

III. Tätigkeiten des Datenschutzbeauftragten 135
1. Entbindung von der Schweigepflicht 135
2. Antwort auf ein Auskunftsverlangen der Aufsichtsbehörde 139
3. Typische auf den Datenschutzbeauftragten des Vertragspartners bezogene Klauseln anderer Verträge 143

C. Dokumentationspflichten im Unternehmen

I. Datenschutzaudit 149

II. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) 171

III. Datenschutz-Folgenabschätzung und Konsultation (Art. 35 f. DS-GVO) 180
1. Übersicht über den Verlauf einer Datenschutz-Folgenabschätzung 182
2. Positiv- und Negativlisten – eine Phänomenologie der Datenschutz-Folgenabschätzung 183
3. Schwellenwertprüfung und Erforderlichkeit einer Datenschutz-Folgenabschätzung 185
4. Durchführung einer Datenschutz-Folgenabschätzung 186
5. Vorherige Konsultation (Art. 36 DS-GVO) 192

IV. Verhaltensregeln und Zertifizierungen 203
1. Ökosystem Audit und akkreditierte Zertifizierungen 203
2. Verhaltensregeln (Art. 40 DS-GVO) 223
3. Zertifizierungen (Art. 42 f. DS-GVO) 241

V. Sicherheit der Verarbeitung und risikobasierter Ansatz 250
1. Ziele der Maßnahmen zur Sicherheit der Verarbeitung 250
2. Einführung zum risikobasierten Ansatz in der DS-GVO 252
3. Schema zur Ermittlung von Risiken der Verarbeitungstätigkeiten 259
4. Verfahren zur Durchführung von Wirksamkeitskontrollen 265
5. Prüfkonzept zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 266

VI. Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 f. DS-GVO) 270
1. Mitteilung an die Aufsichtsbehörde (Art. 33 DS-GVO) 270
2. Mitteilung an die betroffene Person (Art. 34 DS-GVO) 274
3. Dokumentation der Verletzungen des Schutzes personenbezogener Daten (Art. 33 Abs. 5 DS-GVO) 277

VII. Vertraulichkeitspflichten der Beschäftigten 281
1. Verpflichtung zur Vertraulichkeit mit Merkblatt 281
2. Verpflichtung auf das Telekommunikationsgeheimnis mit Merkblatt 293
3. Deklaratorische Belehrung über die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt und Protokoll ... 299

4. Vereinbarung über die Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt und Protokoll 306
5. Vereinbarung zur datenschutzrechtlichen Eingliederung freier Mitarbeiter in den Betrieb des Verantwortlichen 312
6. Vertraulichkeitsvereinbarung für freie Mitarbeiter 319
7. Merkblatt zur Wahrung der Vertraulichkeit in der sozialen Arbeit 342

VIII. Vertreter nach Art. 27 DS-GVO 354
1. Checkliste zu Aufgaben und Umfang des Vertreters nach Art. 27 DS-GVO 354
2. Vertrag über die Benennung eines Vertreters nach Art. 27 DS-GVO .. 358

D. Richtlinien des Unternehmens

I. Konzernrichtlinie der Geschäftsleitung 367
1. Gesellschafterbeschluss zur Einführung einer Datenschutz-Organisation 367
2. Konzernrichtlinie Datenschutz-Organisation 368

II. Unternehmensrichtlinie Datenschutz für Mitarbeiter 374

III. Richtlinien zur Nutzung durch Beschäftigte 393
1. Richtlinie zur Nutzung von Internet und E-Mail 393
2. Richtlinie Homeoffice/Mobile Office (Telearbeit) 426
3. Richtlinie zur Fernwartung durch eigene Mitarbeiter 437
4. Nutzungsvereinbarung zu „Bring Your Own Device" (BYOD) 447
5. Social-Media-Guideline 463

IV. Löschkonzepte 471
1. Aufbewahrungsregeln für ausgewählte Unterlagen 482
2. Löschkonzept 509
3. Löschungsverfahren 518

E. Technische und organisatorische Datensicherheit

I. Überblick: Rationalisierung von Datenschutzthemen im Unternehmen .. 529
1. Methodischer Aufbau 529
2. Richtlinien zur Ermittlung von Schnittmengen zu anderen Funktionen 551
3. Checkliste der Rollen und ihrer Funktionen 561
4. Tabellarische Aufstellung von Rollenüberdeckungen 572
5. Vermeidung unrationeller Arbeitsweisen..... 585

II. Technische und organisatorische Maßnahmen (Art. 32, 25 DS-GVO) ... 599
1. Anwendung bei interner Verarbeitung und Auftragsverarbeitung 599
2. Formular zur Prüfung der technischen und organisatorischen Maßnahmen 603
3. Vereinfachte Risikobewertung nach Angemessenheitsprinzip für KMU und Vereine 643

III. Prüfkontrolle 667

IV. Formular zur Prüfung von Berechtigungskonzepten 675
V. Datenschutz im Krisen- und Notfallmanagement 685

F. Rechte der betroffenen Person

I. Informationspflichten bei Erhebung von personenbezogenen Daten (Art. 13 f. DS-GVO) 705
1. Datenschutzerklärung für Websites 706
2. Datenschutzerklärung für mobile Apps 726
3. Besondere Nutzungsformen von Websites 736
4. Newsletter 749
5. Web Analytics 755
6. Social Media 771
7. Online-Werbung 781
II. Auskunftsrecht der betroffenen Person (Art. 15 DS-GVO) 797
1. Auskunftsverlangen der betroffenen Person 797
2. Antwort auf Auskunftsverlangen mit Recht auf Kopie (Art. 15 DS-GVO) 803
III. Recht auf Berichtigung (Art. 16 DS-GVO) 811
1. Berichtigungsverlangen des Betroffenen 811
2. Antwort des Verantwortlichen an den Betroffenen 814
IV. Rechte auf Löschung und Mitteilung (Art. 17, 19 DS-GVO) 818
1. Recht auf Löschung und „Recht auf Vergessenwerden" (Art. 17 DS-GVO) 818
2. Informationspflicht an Dritte bei einem Löschungsersuchen (Art. 17 Abs. 2 DS-GVO) 822
V. Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) 827
1. Verlangen des Betroffenen 827
2. Antwort des Verantwortlichen an den Betroffenen 830
VI. Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) 831
1. Verlangen des Betroffenen 831
2. Antwort des Verantwortlichen an den Betroffenen 834

G. Zusammenarbeit mit anderen Unternehmen

I. Vereinbarung der Auftragsverarbeitung (Art. 28 f. DS-GVO) 837
1. Abgrenzung von Auftragsverarbeitung und gemeinsamer Verantwortung 837
2. Richtlinie Auftragsverarbeitung 843
3. Prüfliste vor Vertragsabschluss einer Auftragsverarbeitung 852
4. Vertragsmuster Auftragsverarbeitung 858
5. Maßnahmenübersicht und deren risikobasierte Bewertung bei der Auftragsverarbeitung 880
II. Formulare während der Laufzeit der Auftragsverarbeitung (Art. 28 DS-GVO) 890
1. Genehmigung von Unterauftragnehmern 890
2. Änderung bei den Weisungsberechtigten/-empfängern 892

3. Änderung beim Datenschutzbeauftragten ... 894
4. Änderungen in den Verfahren ... 896
5. Meldebogen Datenschutz- oder IT-Sicherheitsvorfall im Innenverhältnis ... 897
6. Prüfliste für Auftragsverarbeitung bei Insolvenz des Auftraggebers/Auftragnehmers ... 905

III. Fernwartung durch Drittunternehmen ... 909
1. Anlage zur Fernwartung für externe Dienstleister ... 910
2. Datenschutzvereinbarung für den Remotezugriff ... 922
3. Allgemeine Bestimmungen ... 923
4. Arbeitsanweisung zur Fernwartung für Dienstleister ... 924

IV. Vertraulichkeitsvereinbarungen ... 927
1. Vertraulichkeitsvereinbarung bei Dienstleistungsverträgen ... 927
2. Vertraulichkeitsvereinbarung bei M&A-Transaktionen ... 937

V. Gemeinsam für die Verarbeitung Verantwortliche (Art. 26 DS-GVO) ... 957
1. Prüftabelle gemeinsam für die Verarbeitung Verantwortliche ... 961
2. Vereinbarung über die gemeinsame Verantwortung ... 967
3. Informationsblatt für betroffene Personen ... 979

VI. Einsatz von Cloud Computing im Unternehmen ... 981

VII. Datentransfers in Drittstaaten ... 995
1. Übersicht über internationale Datentransfers (Art. 44 ff. DS-GVO) ... 995
2. Anhänge zu den Standarddatenschutzklauseln ... 1005
3. Binding Corporate Rules ... 1013
4. Einwilligung der betroffenen Personen ... 1028
5. Antrag auf Genehmigung des Transfers personenbezogener Daten in ein Drittland ohne ausreichendes Datenschutzniveau (Art. 46 Abs. 3 DS-GVO) ... 1039

H. Beschäftigtendatenschutz

I. Einwilligung durch Beschäftigte ... 1043
1. Einwilligungserklärung zur Veröffentlichung von Mitarbeiterfotos ... 1043
2. Einwilligungserklärung zur Speicherung von Bewerberdaten ... 1050

II. Beschäftigtendatenschutz bei Arbeitsunfähigkeit und betrieblichem Eingliederungsmanagement (BEM) ... 1060
1. Betriebsvereinbarung zu Kranken- und BEM-Unterlagen ... 1068
2. Einladungsschreiben zum BEM ... 1091

III. Videoüberwachung auf Firmengeländen ... 1097
1. Checkliste zur Videoüberwachung ... 1099
2. Richtlinie und Betriebsvereinbarung zur Videoüberwachung im Betrieb ... 1102
3. Festlegungen vor Inbetriebnahme der Videoüberwachung ... 1124
4. Maßnahmen zum Schutz der betroffenen Personen ... 1129
5. Protokoll zur Auswertung von Videoaufnahmen ... 1132
6. Checkliste zur Videoüberwachung für KMU und Vereine ... 1133

IV. Tor- und Spindkontrollen bei Beschäftigten 1135
1. Checkliste zu Tor- und Spindkontrollen 1137
2. Betriebsvereinbarung über die Durchführung von Tor- und Spindkontrollen 1138

V. Detektiveinsatz gegen Beschäftigte 1149

VI. Betriebsvereinbarung zum Terrorlisten-Screening 1158

VII. Screening von Beschäftigten 1175
1. Kontrollmöglichkeiten der betrieblichen E-Mail-Kommunikation 1175
2. Checkliste zur Zweckänderung 1190
3. Information der betroffenen Person 1195
4. Protokollierung der Einsichtnahme 1202

I. Kundendatenschutz

I. Organisation des Kundendatenschutzes 1205

II. Einwilligungen durch betroffene Personen 1215

III. Einwilligung in Werbeversand/Newsletter 1226

IV. Bonitätsprüfung von natürlichen Personen 1241
1. Bonitätsprüfung und Informationen bei Kaufverträgen 1243
2. Darlehen-Selbstauskunft 1252
3. Mieter-Selbstauskunft 1260
4. Haushaltsrechnung von natürlichen Personen 1269

V. Checkliste bei polizeilichen Auskunftsverlangen 1272

VI. Mehrparteien-Vereinbarung zwischen gemeinsam Verantwortlichen bei Online-Angeboten 1287

J. Datenschutz und Personenbildnisse

I. Datenschutz bei Nutzung von Personenbildnissen 1303

II. Checkliste Einwilligungserklärung bei Nutzung von Fotos- oder Videoaufnahmen 1312

III. Model-Release-Vereinbarung 1317

IV. Datenschutzinformation für Bildnisnutzung 1321

K. Gesundheitsdatenschutz

I. Zusammenspiel der Akteure im Gesundheitsbereich 1325
1. Checkliste zum datenschutzrechtlichen Vertragsmanagement für Apotheken 1327
2. Vereinbarung zur Datenübermittlung zwischen Arzt und medizinischem Laborarzt 1331

II. Datenschutzrechtliche Einwilligung im Gesundheitsbereich 1340
1. Einverständnis in die Erstellung der Honorarrechnung und den Einzug inkl. Abtretung der Honorarforderung an zahnärztliche Abrechnungsgesellschaft 1340

2. Datenschutzrechtliche Einwilligungserklärung in die Verarbeitung von personenbezogenen Daten zur Anlage einer Kundenkarte 1346
3. Zustimmung zur Datenübermittlung an den Hausarzt sowie vom Hausarzt an andere Leistungserbringer 1350
III. Transparenz und Informationspflichten 1354
1. Datenschutzinformationen über die Verarbeitung von Kundendaten in der Apotheke 1354
2. Richtlinie zu Datenschutz und Datensicherheit in der Apotheke 1367
IV. Datenschutz in der klinischen und nichtklinischen Forschung 1377
1. Checkliste zum Datenschutz in der klinischen und nichtklinischen Forschung 1380
2. Vertragsklauseln Auftragsverarbeitung Sponsor/CRO 1381
3. Vertragsklausel gemeinsam Verantwortliche 1385
4. Vertragsklausel getrennt Verantwortliche 1390

L. Datenschutz in Vereinen, Verbänden und Stiftungen

I. Rundschreiben an Mitgliedsverbände durch Dachverband 1396
II. Merkblatt Datenschutz für den Vorstand 1401
III. Vertraulichkeitsverpflichtung für Vorstände 1404
IV. Datenschutzerklärung für Mitglieder 1406
V. Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO 1414

M. Datenschutz in der Anwaltskanzlei

I. Merkblatt und Verschwiegenheitserklärung zu Datenschutz und Mandantengeheimnis für Angestellte 1423
II. Datenschutzerklärung für Mandanten 1428
III. Verarbeitungsverzeichnis mit Musterverfahren 1435
IV. Einsatz von Dienstleistern, beA und Legal-Tech-Produkten 1440

N. Behördliches und verwaltungsgerichtliches Verfahren

I. Eingabe an eine Aufsichtsbehörde 1449
II. Antrag auf Wiederherstellung der aufschiebenden Wirkung 1455
III. Klage gegen eine Anordnung der Aufsichtsbehörde 1462
IV. Einstweiliger Rechtsschutz gegen Informationstätigkeit der Aufsichtsbehörde 1467

O. Strafverfahren und Ordnungswidrigkeiten

I. Übersicht Sanktionen 1477
II. Anträge auf Akteneinsicht 1504
1. Antrag auf Akteneinsicht des Beschuldigten 1504
2. Antrag auf Akteneinsicht als Verletzter gem. § 406e StPO/§ 475 StPO 1509
3. Abwehr eines Akteneinsichtsantrags 1518

III. Einspruch gegen Bußgeldbescheid 1520
IV. Beschwerde gegen Durchsuchungs- und Beschlagnahmebeschluss 1531
V. Checkliste: Verhaltensempfehlung bei Durchsuchungen 1540
VI. Anträge auf Einstellung 1550
1. Antrag auf Einstellung gem. § 170 Abs. 2 StPO (ggf. iVm § 46 Abs. 1 OWiG und ggf. iVm § 41 BDSG) 1551
2. Antrag auf Einstellung gem. § 47 OWiG (ggf. iVm § 41 BDSG) (aus Opportunitätsgründen) 1555

P. Datenschutz in Österreich

I. Datengeheimnis (= Mitarbeiterverpflichtungserklärung) 1559
II. Bildverarbeitung/Videoüberwachung 1570
III. Blacklist zur Datenschutz-Folgenabschätzung 1583
IV. Antrag an die DSB zur Genehmigung von Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke 1588

Sachverzeichnis 1595