

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	20
III. Datenschutzorganisation im Unternehmen	25
1. Organisatorischer und strategischer Aufbau	25
2. Pflichtübung, Kür oder Privacy-Manager: Vom Datenschutzbeauftragten zu Datenschutz-Compliance	32
3. Dienstleister oder Kontrolleur: Die zwei Gesichter von Datenschutzabteilungen	37
4. Von der Auftragsverarbeitung bis zur Verbandsarbeit: Zuständigkeitsbereiche im Einzelnen	41
5. Risikoverständnis und Reifegrad einer Datenschutzorganisation	45
6. Umgang mit Anfragen und Audits der Aufsichtsbehörden	48
7. Arbeitsweise am Beispiel Datenschutz-Folgenabschätzung: Dienst nach Vorschrift oder Teamarbeit	52
IV. Code of Conduct und Selbstverpflichtung zum Datenschutz	60
1. Datenschutz im Code of Conduct	60
2. Übersicht zu Hinweisgebersystemen und Meldestellen (Whistleblower-Hotlines)	63
3. Meldestelle und Hinweisgebersystem (Whistleblower-Hotline) im Code of Conduct	73
4. Datenschutzerklärung für ein elektronisches Hinweisgeberportal	74
5. Interne Richtlinie zum Einsatz eines Hinweisgebersystems	76
6. Internal Investigations: Unternehmenspflicht vs. Datenschutz	85

B. Der Datenschutzbeauftragte

I. Benennung und Abberufung des Datenschutzbeauftragten	89
1. Benennung als Datenschutzbeauftragter	89
2. Abberufung durch den Arbeitgeber	109

II. Verträge mit externen Datenschutzbeauftragten	116
1. Dienstvertrag mit einem externen Datenschutzbeauftragten	116
2. Beratungsvertrag mit einem Dienstleistungsunternehmen	135
3. Aufhebungsvertrag der Parteien	146
III. Tätigkeiten des Datenschutzbeauftragten	149
1. Entbindung von der Schweigepflicht	149
2. Antwort auf ein Auskunftsverlangen der Aufsichtsbehörde	152
3. Typische auf den Datenschutzbeauftragten des Vertragspartners be- zogene Klauseln anderer Verträge	156
C. Dokumentationspflichten im Unternehmen	
I. Datenschutzaudit	163
II. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)	186
III. Datenschutz-Folgenabschätzung und Konsultation (Art. 35 f. DS-GVO)	195
1. Übersicht über den Verlauf einer Datenschutz-Folgenabschätzung	197
2. Positiv- und Negativlisten – eine Phänomenologie der Datenschutz- Folgenabschätzung	198
3. Schwellenwertprüfung und Erforderlichkeit einer Datenschutz-Fol- genabschätzung	199
4. Durchführung einer Datenschutz-Folgenabschätzung	201
5. Vorherige Konsultation (Art. 36 DS-GVO)	207
IV. Verhaltensregeln und Zertifizierungen	218
1. Ökosystem Audit und akkreditierte Zertifizierungen	218
2. Verhaltensregeln (Art. 40 DS-GVO)	239
3. Zertifizierungen (Art. 42 f. DS-GVO)	259
V. Sicherheit der Verarbeitung und risikobasierter Ansatz	267
1. Ziele der Maßnahmen zur Sicherheit der Verarbeitung	267
2. Einführung zum risikobasierten Ansatz in der DS-GVO	270
3. Schema zur Ermittlung von Risiken der Verarbeitungstätigkeiten	276
4. Verfahren zur Durchführung von Wirksamkeitskontrollen	282
5. Prüfkonzert zu Datenschutz durch Technikgestaltung und durch da- tenschutzfreundliche Voreinstellungen	284
VI. Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 f. DS-GVO)	287
1. Mitteilung an die Aufsichtsbehörde (Art. 33 DS-GVO)	287
2. Mitteilung an die betroffene Person (Art. 34 DS-GVO)	291
3. Dokumentation der Verletzungen des Schutzes personenbezogener Daten (Art. 33 Abs. 5 DS-GVO)	295
VII. Vertraulichkeitspflichten der Beschäftigten	298
1. Verpflichtung zur Vertraulichkeit mit Merkblatt	298
2. Verpflichtung auf das Telekommunikationsgeheimnis mit Merkblatt .	310
3. Deklaratorische Belehrung über die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt und Protokoll	317
4. Vereinbarung über die Wahrung von Geschäftsgeheimnissen mit Merkblatt	324

5. Vereinbarung zur datenschutzrechtlichen Eingliederung freier Mitarbeiter in den Betrieb des Verantwortlichen	330
6. Vertraulichkeitsvereinbarung für freie Mitarbeiter	337
7. Merkblatt zur Wahrung der Vertraulichkeit in der sozialen Arbeit	361
VIII. Vertreter nach Art. 27 DS-GVO	373
1. Checkliste zu Aufgaben und Umfang des Vertreters nach Art. 27 DS-GVO	373
2. Vertrag über die Benennung eines Vertreters nach Art. 27 DS-GVO ...	377

D. Richtlinien des Unternehmens

I. Konzernrichtlinie der Geschäftsleitung	387
1. Gesellschafterbeschluss zur Einführung einer Datenschutz-Organisation	387
2. Konzernrichtlinie Datenschutz-Organisation	388
II. Unternehmensrichtlinie Datenschutz für Mitarbeiter	395
III. Richtlinien zur Nutzung durch Beschäftigte	414
1. Richtlinie zur Nutzung von Internet, E-Mail und anderen elektronischen Kommunikationsmitteln	414
2. Richtlinie Homeoffice/Mobile Office (Tearbeit)	450
3. Richtlinie zur Fernwartung durch eigene Mitarbeiter	462
4. Nutzungsvereinbarung zu „Bring Your Own Device“ (BYOD)	472
5. Social-Media-Guideline	489
IV. Löschkonzepte	499
1. Aufbewahrungsregeln für ausgewählte Unterlagen	513
2. Löschkonzept	544
3. Lösungsverfahren	564

E. Technische und organisatorische Datensicherheit

I. Überblick: Rationalisierung von Datenschutzthemen im Unternehmen .	575
1. Methodischer Aufbau	576
2. Richtlinien zur Ermittlung von Schnittmengen zu anderen Funktionen	600
3. Checkliste der Rollen und ihrer Funktionen	610
4. Tabellarische Aufstellung von Rollenüberdeckungen	621
5. Vermeidung unrationeller Arbeitsweisen.....	634
II. Technische und organisatorische Maßnahmen (Art. 32, 25 DS-GVO) ...	648
1. Anwendung bei interner Verarbeitung und Auftragsverarbeitung	648
2. Formular zur Prüfung der technischen und organisatorischen Maßnahmen	652
3. Vereinfachte Risikobewertung nach Angemessenheitsprinzip für KMU und Vereine	697
III. Prüfkontrolle	722
IV. Formular zur Prüfung von Berechtigungskonzepten	730
V. Datenschutz im Krisen- und Notfallmanagement	740

F. Rechte der betroffenen Person

I. Informationspflichten bei Erhebung von personenbezogenen Daten (Art. 13 f. DS-GVO)	759
1. Datenschutzerklärung für Websites	760
2. Datenschutzerklärung für mobile Apps	779
3. Besondere Nutzungsformen von Websites	790
4. Newsletter	804
5. Web Analytics	810
6. Social Media	825
7. Online-Werbung	835
II. Auskunftsrecht der betroffenen Person (Art. 15 DS-GVO)	851
1. Auskunftsverlangen der betroffenen Person	851
2. Antwort auf Auskunftsverlangen mit Recht auf Kopie (Art. 15 DS-GVO)	859
III. Recht auf Berichtigung (Art. 16 DS-GVO)	870
1. Berichtigungsverlangen des Betroffenen	870
2. Antwort des Verantwortlichen an den Betroffenen	874
IV. Rechte auf Löschung und Mitteilung (Art. 17, 19 DS-GVO)	878
1. Recht auf Löschung und „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)	878
2. Informationspflicht an Dritte bei einem Löschungsersuchen (Art. 17 Abs. 2 DS-GVO)	882
V. Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)	887
1. Verlangen des Betroffenen	887
2. Antwort des Verantwortlichen an den Betroffenen	890
VI. Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)	892
1. Verlangen des Betroffenen	892
2. Antwort des Verantwortlichen an den Betroffenen	895

G. Zusammenarbeit mit anderen Unternehmen

I. Vereinbarung der Auftragsverarbeitung (Art. 28 f. DS-GVO)	897
1. Abgrenzung von Auftragsverarbeitung und gemeinsamer Verantwortung	897
2. Richtlinie Auftragsverarbeitung	904
3. Prüfliste vor Vertragsabschluss einer Auftragsverarbeitung	913
4. Vertragsmuster Auftragsverarbeitung	919
5. Maßnahmenübersicht und deren risikobasierte Bewertung bei der Auftragsverarbeitung	942
6. Standardvertragsklauseln der EU-Kommission für Auftragsverarbeitungsverträge mit Ergänzungsklauseln	951
7. Checkliste zur Prüfung von Auftragsverarbeitungsverträgen	987
II. Formulare während der Laufzeit der Auftragsverarbeitung (Art. 28 DS-GVO)	1018
1. Genehmigung von Unterauftragnehmern	1018
2. Änderung bei den Weisungsberechtigten/-empfängern	1021

Inhaltsverzeichnis	XI
3. Änderung beim Datenschutzbeauftragten	1022
4. Änderungen in den Verfahren	1024
5. Meldebogen Datenschutz- oder IT-Sicherheitsvorfall im Innenverhältnis	1025
6. Prüfliste für Auftragsverarbeitung bei Insolvenz des Auftraggebers/Auftragnehmers	1033
III. Fernwartung durch Drittunternehmen	1038
1. Anlage zur Fernwartung für externe Dienstleister	1039
2. Datenschutzvereinbarung für den Remotezugriff	1051
3. Allgemeine Bestimmungen	1052
4. Arbeitsanweisung zur Fernwartung für Dienstleister	1053
IV. Vertraulichkeitsvereinbarungen	1056
1. Vertraulichkeitsvereinbarung bei Dienstleistungsverträgen	1056
2. Vertraulichkeitsvereinbarung bei M&A-Transaktionen	1066
V. Gemeinsam für die Verarbeitung Verantwortliche (Art. 26 DS-GVO)	1086
1. Prüftabelle gemeinsam für die Verarbeitung Verantwortliche	1090
2. Vereinbarung über die gemeinsame Verantwortung	1097
3. Informationsblatt für betroffene Personen	1107
VI. Einsatz von Cloud Computing im Unternehmen	1109
1. Checklisten zur Cloud-Nutzung und zu Besonderheiten bei Auftragsvereinbarung und Auftragsverarbeitungsvereinbarung	1109
2. Freigabe und Einsatz von Software as a Service am Beispiel von Microsoft 365	1127
VII. Datentransfers in Drittstaaten	1138
1. Übersicht über internationale Datentransfers (Art. 44 ff. DS-GVO)	1138
2. Standardvertragsklauseln	1149
3. Binding Corporate Rules	1161
4. Einwilligung der betroffenen Personen	1176
5. Antrag auf Genehmigung des Transfers personenbezogener Daten in ein Drittland ohne ausreichendes Datenschutzniveau (Art. 46 Abs. 3 DS-GVO)	1188
 H. Beschäftigtendatenschutz	
I. Einwilligung durch Beschäftigte	1191
1. Einwilligungserklärung zur Veröffentlichung von Mitarbeiterfotos	1191
2. Einwilligungserklärung zur Speicherung von Bewerberdaten	1200
II. Beschäftigtendatenschutz bei Arbeitsunfähigkeit und betrieblichem Eingliederungsmanagement (BEM)	1210
1. Betriebsvereinbarung zu Kranken- und BEM-Unterlagen	1221
2. Einladungsschreiben zum BEM	1244
III. Videoüberwachung auf Firmengeländen	1250
1. Checkliste zur Videoüberwachung	1253
2. Richtlinie und Betriebsvereinbarung zur Videoüberwachung im Betrieb	1257
3. Festlegungen vor Inbetriebnahme der Videoüberwachung	1279
4. Maßnahmen zum Schutz der betroffenen Personen	1284

5. Protokoll zur Auswertung von Videoaufnahmen	1286
6. Checkliste zur Videoüberwachung für KMU und Vereine	1287
IV. Tor- und Spindkontrollen bei Beschäftigten	1290
1. Checkliste zu Tor- und Spindkontrollen	1292
2. Betriebsvereinbarung über die Durchführung von Tor- und Spindkontrollen	1294
V. Detektiveinsatz gegen Beschäftigte	1304
VI. Betriebsvereinbarung zum Terrorlisten-Screening	1315
VII. Screening von Beschäftigten	1331
1. Kontrollmöglichkeiten der betrieblichen E-Mail-Kommunikation	1331
2. Checkliste zur Zweckänderung	1349
3. Information der betroffenen Person	1354
4. Protokollierung der Einsichtnahme	1361
VIII. Rahmenbetriebsvereinbarung IT-Systeme	1365

I. Kundendatenschutz

I. Organisation des Kundendatenschutzes	1395
II. Einwilligungen durch betroffene Personen	1405
III. Einwilligung in Werbeversand/Newsletter	1417
IV. Bonitätsprüfung von natürlichen Personen	1433
1. Bonitätsprüfung und Informationen bei Kaufverträgen	1435
2. Darlehen-Selbstauskunft	1445
3. Mieter-Selbstauskunft	1453
4. Haushaltsrechnung von natürlichen Personen	1462
V. Checkliste bei polizeilichen Auskunftsverlangen	1465
VI. Mehrparteien-Vereinbarung zwischen gemeinsam Verantwortlichen bei Online-Angeboten	1479
VII. Datenschutzerklärung für Kunden	1497

J. Datenschutz und Personenbildnisse

I. Datenschutz bei Nutzung von Personenbildnissen	1503
II. Checkliste Einwilligungserklärung bei Nutzung von Foto- oder Videoaufnahmen	1512
III. Model-Release-Vereinbarung	1517
IV. Datenschutzinformation für Bildnisnutzung	1521

K. Gesundheitsdatenschutz

I. Zusammenspiel der Akteure im Gesundheitsbereich	1525
1. Checkliste zum datenschutzrechtlichen Vertragsmanagement für Apotheken	1528
2. Vereinbarung zur Datenübermittlung zwischen Arzt und medizinischem Laborarzt	1532

II. Datenschutzrechtliche Einwilligung im Gesundheitsbereich	1541
1. Einverständnis in die Erstellung der Honorarrechnung und den Einzug inklusive Abtretung der Honorarforderung an zahnärztliche Abrechnungsgesellschaft	1541
2. Datenschutzrechtliche Einwilligungserklärung in die Verarbeitung von personenbezogenen Daten zur Anlage einer Kundenkarte	1548
3. Zustimmung zur Datenübermittlung an den Hausarzt sowie vom Hausarzt an andere Leistungserbringer	1551
III. Transparenz und Informationspflichten	1555
1. Datenschutzinformationen über die Verarbeitung von Kundendaten in der Apotheke	1555
2. Richtlinie zu Datenschutz und Datensicherheit in der Apotheke	1568
IV. Datenschutz in der klinischen und nichtklinischen Forschung	1580
1. Checkliste zum Datenschutz in der klinischen und nichtklinischen Forschung	1583
2. Vertragsklauseln Auftragsverarbeitung Sponsor/CRO	1584
3. Vertragsklausel gemeinsam Verantwortliche	1588
4. Vertragsklausel getrennt Verantwortliche	1594

L. Datenschutz in Vereinen, Verbänden und Stiftungen

I. Rundschreiben an Mitgliedsverbände durch Dachverband	1600
II. Merkblatt Datenschutz für den Vorstand	1605
III. Vertraulichkeitsverpflichtung für Vorstände	1608
IV. Datenschutzerklärung für Mitglieder	1610
V. Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO	1618

M. Datenschutz in der Anwaltskanzlei

I. Merkblatt und Verschwiegenheitserklärung zu Datenschutz und Mandatengeheimnis für Angestellte	1628
II. Datenschutzerklärung für Mandanten	1633
III. Verarbeitungsverzeichnis mit Musterverfahren	1640
IV. Einsatz von Dienstleistern, beA und Legal-Tech-Produkten	1645

N. Behördliches und verwaltungsgerichtliches Verfahren

I. Eingabe an eine Aufsichtsbehörde	1653
II. Antrag auf Wiederherstellung der aufschiebenden Wirkung	1659
III. Klage gegen eine Anordnung der Aufsichtsbehörde	1666
IV. Einstweiliger Rechtsschutz gegen die Informationstätigkeit der Aufsichtsbehörde	1671

O. Strafverfahren und Ordnungswidrigkeiten

I. Tabellarische Übersichten zu Sanktionsnormen 1685

1. Sanktionsnormen und Anwendungsvorschriften des supranationalen
Regelungsregimes 1685

2. Sanktionsnormen und Anwendungsvorschriften des nationalen Rege-
lungsregimes 1707

II. Anträge auf Akteneinsicht 1716

1. Antrag auf Akteneinsicht des Beschuldigten 1716

2. Antrag auf Akteneinsicht als Verletzter gem. § 406e StPO/§ 475 StPO 1721

3. Abwehr eines Akteneinsichtsanspruchs 1728

III. Anträge auf Einstellung 1730

1. Antrag auf Einstellung gem. § 170 Abs. 2 StPO (ggf. iVm § 46 Abs. 1
OWiG und ggf. iVm § 41 BDSG) 1731

2. Antrag auf Einstellung gem. § 47 OWiG (ggf. iVm § 41 BDSG) aus
Opportunitätsgründen 1735

IV. Einspruch gegen Bußgeldbescheid 1739

V. Checkliste: Verhaltensempfehlung bei Durchsuchungen 1747

VI. Beschwerde gegen Durchsuchungs- und Beschlagnahmebeschluss 1757

P. Datenökonomie und Datenschutz

I. Data Act/Datenverordnung 1765

II. Datenlizenz 1781

Q. Künstliche Intelligenz

I. Checkliste zur Anwendbarkeit der KI-Verordnung 1800

II. Checkliste zur Einordnung der Pflichten nach der KI-Verordnung 1805

III. Vergleich der Pflichten nach der KI-VO und der DS-GVO 1820

1. Normen der DS-GVO mit Bestimmungen der KI-VO 1820

2. Normen der KI-VO mit Einfluss auf datenschutzrechtliche Normen 1823

R. Datenschutz in Österreich

I. Datengeheimnis (= Mitarbeiterverpflichtungserklärung) 1827

II. Bildverarbeitung/Videoüberwachung 1838

III. Blacklist zur Datenschutz-Folgenabschätzung 1851

IV. Antrag an die DSB zur Genehmigung von Verarbeitung für im öffentli-
chen Interesse liegende Archivzwecke, wissenschaftliche oder historische
Forschungszwecke oder statistische Zwecke 1856

Sachverzeichnis 1863