

Inhaltsverzeichnis

Vorwort.....	5
Abkürzungsverzeichnis/Quellenverzeichnis.....	21
Verzeichnis ausgewählter Literatur.....	25
Verzeichnis der Checklisten.....	27
1. Datenschutz in Deutschland	29
a. Was regelt die Europäische Datenschutz-Grundverordnung?.....	30
b. Gefährdungslage	31
c. Gesetzliche Grundlagen des Datenschutzes in Deutschland	36
d. Datenschutzziele	37
e. Anwendungsbereich und Marktortprinzip	39
f. Datenschutzregelungen.....	39
g. Datenschutz in der Bundesverwaltung.....	42
h. Aufbau der DSGVO.....	42
i. Aufbau des BDSG	47
j. Wann gilt welches Gesetz? DSGVO und BDSG richtig einsetzen!	49
2. Datenschutzgesetze konkret	55
a. Grundsätze beim Datenschutz nach der DSGVO.....	55
b. Begriffe in der DSGVO und im BDSG und ihre Bedeutung.....	61
c. Alles, was nicht ausdrücklich erlaubt ist, ist verboten	67
d. Verantwortlicher, gemeinsam Verantwortliche.....	67
e. Beschäftigtendaten.....	68
f. Kategorien personenbezogener Daten, betroffene Personen und Empfänger	69
g. Besondere Kategorien personenbezogener Daten	70
h. Speicherdauer.....	71

Inhaltsverzeichnis

i.	Auftragsverarbeitung.	71
j.	Verzeichnis der Verarbeitungstätigkeiten.	72
k.	Datenschutz-Folgenabschätzung (DSFA).	77
l.	Datenübermittlung ins Ausland.	78
m.	Datenschutz durch Technikgestaltung und datenschutzfreundliche Einstellungen	81
n.	Sicherung der Verarbeitung. Technische und organisatorische Maßnahmen (TOM)	83
o.	Videoüberwachung	87
p.	Aktualisierungen	90
q.	Sanktionen bei Verstößen.	90
r.	Keine Bußgelder gegen Behörden und öffentliche Stellen, aber Ausnahmen	92
s.	Persönliche Strafen bei Datenschutzverstößen	94
t.	Datenschutzpannen.	94
3.	Rechte der Betroffenen	96
a.	Informationspflichten des Arbeitgebers.	96
aa.	Informationspflicht bei der Erhebung personenbezogener Daten bei der betroffenen Person	97
bb.	Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden	98
b.	Information nach Datenschutzpannen.	99
c.	Auskunftsrecht Betroffener	100
d.	Wie müssen die Informationen aussehen?	102
e.	Übersicht über Regelungen und Ausnahmen bei der Informationspflicht und Auskunftsrechte	103
f.	Recht auf Berichtigung	109
g.	Recht auf Löschung («Recht auf Vergessenwerden»)	110
h.	Einschränkung der Verarbeitung.	111
i.	Mitteilungspflicht bei Berichtigung, Einschränkung oder Löschung	112
j.	Recht auf Datenübertragbarkeit.	112
k.	Widerspruchsrecht.	113
l.	Recht auf Widerruf einer Einwilligung.	114
m.	Recht auf nicht-automatisierte Entscheidung	114
n.	Rechte gegenüber der Aufsichtsbehörde	115
o.	Recht auf Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	115

4.	Beschäftigtendatenschutz – die Präzisierung durch den § 26 BDSG	116
5.	Kontrolle des Datenschutzes durch die gesetzliche Interessenvertretung	121
a.	Datenschutz und Mitbestimmungsrechte	121
b.	Beteiligungsrechte und andere Rechtsvorschriften zur Sicherung des Beschäftigtendatenschutzes für Betriebs- und Personalräte	123
c.	Landesdatenschutzgesetze	131
d.	Sachverständige	131
6.	BeDaX – Datenschutz in Betrieb und Verwaltung prüfen.	134
7.	Aufsichtsbehörden beim Datenschutz	138
8.	Betriebliche und behördliche Datenschutzbeauftragte (DSB)	139
a.	Bestellung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten	140
b.	Gemeinsamer Datenschutzbeauftragter	141
c.	Wer kann Datenschutzbeauftragter werden?	142
d.	Stellung des betrieblichen bzw. behördlichen Datenschutzbeauftragten	142
e.	Mitbestimmungsrechte bei der Bestellung oder Abberufung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten	143
f.	Aufgaben eines betrieblichen bzw. behördlichen Datenschutzbeauftragten	144
g.	Hilfskräfte des DSB, Datenschutzkoordinatoren und technischer Datenschutz	145
9.	Datenschutz im Büro der Interessenvertretung	152
a.	Betriebs- und Personalrat keine Verantwortlichen im Datenschutz	152
b.	Kontrolle des Betriebs- und Personalrats durch den Datenschutzbeauftragten	155
c.	Ihr habt kein Datenschutzkonzept? Dann bekommt ihr die Daten nicht!	159

10. Der Weg zum Datenschutzkonzept der Interessenvertretung in sechs Schritten	161
a. Der »Sonderbeauftragte für den Datenschutz« (SfD) – der Datenschutzspezialist der gesetzlichen Interessenvertretung	162
b. Welche Daten darf die Interessenvertretung verarbeiten?	164
c. Personenbezogene Daten der Belegschaft dauerhaft speichern?	167
d. Personenbezogene E-Mails der Interessenvertretung	169
e. Das Datenschutzkonzept der Interessenvertretung	173
f. Datenschutz-Bestandsaufnahme (Audit) im Gremium	174
g. Keine Verarbeitungsverzeichnisse, aber eine Nachweisliste	182
h. Verzeichnis der Verarbeitungstätigkeiten/Nachweisliste	184
i. Muster: Verzeichnis der Verarbeitungstätigkeiten/ Nachweisliste im Gremium	187
j. Löschkonzept in der Praxis	194
k. Technische und organisatorische Maßnahmen (TOM)	196
l. Organisationslösungen für das Büro der Interessenvertretung	198
m. »Geschäftsordnung Datenschutz« – das Datenschutzkonzept des Betriebs- oder Personalrats	200
n. Elemente einer »Geschäftsordnung Datenschutz« für eine kleine gesetzliche Interessenvertretung	200
o. Die halbjährliche Kontrolle des Umgangs mit personenbezogenen Daten im Gremium	207
p. Einwilligungserklärung für die Interessenvertretung	208
q. Muster-Einwilligung	209
r. Widerruf zur Einwilligungserklärung Nr. XXXX/XX	212
s. Aktennotiz über die Vernichtung der Einwilligungserklärung	212
11. Datenschutz in der Schwerbehindertenvertretung (SBV)	214
12. Datenschutz beim Betrieblichen Eingliederungsmanagement (BEM)	218
13. Datenschutz in der Jugend- und Auszubildendenvertretung (JAV)	225

14. Datenschutz und Hinweisgeberschutzgesetz (HinSchG) . .	226
15. Künstliche Intelligenz (KI)	233
16. Künstliche Intelligenz im Einsatz: ChatGPT	235
17. Homeoffice	239
18. Blickschutz: Unterwegs und im Homeoffice	243
19. Videokonferenzen.	247
20. Standard-Datenschutzmodell (SDM).	252
21. IT-Grundschutz	253
22. Angriffe von außen und innen.	256
a. Das Firmennetzwerk	259
b. Kontrolle über das Netzwerk	260
c. Sicherheitsrisiko »Sniffer«	262
aa. Das Ausschnüffeln konkret	262
bb. Sniffer abwehren	264
d. WLAN	266
e. VPN – der Sicherheitstunnel	267
f. Thin Client/Cloud	268
g. Überwachung durch das Betriebssystem	269
h. Zugriff des Systemverwalters auf sensible Daten	269
i. Fazit	270
23. Überwachen und Ausspionieren.	271
a. Hintertür-, Fernwartungs- und Kontrollprogramme	271
aa. Die Hintertürprogramme	273
bb. Die wichtigsten Schnüffelfunktionen der Hackertools	273
cc. Gegenwehr	275
b. Die Fernwartungsprogramme	275
c. Bot-Netze	276
d. Der Chef liest mit – Überwachungsprogramme	277
aa. Big Brother im Betrieb	277
bb. Die Praxis	281
e. Kontrollprogramme entdecken	282

Inhaltsverzeichnis

f.	Überwachungssoftware auf Smartphones	283
aa.	Totale Kontrolle von Smartphones	283
bb.	Auswerten der Daten	285
cc.	Rechtliche Fragen	286
dd.	Was tun?	287
g.	Alles rechtens?	288
24.	Windows-Datenschutz	291
a.	Datenschleuder Windows 11	291
b.	Windows-Benutzerkonten	296
25.	Die »Brandschutzmauer« zum Internet	298
a.	Die eingebaute Firewall in Windows	298
b.	Protokolle einer Firewall	299
c.	Fazit	300
26.	Seuchengefahr: Computerviren	301
a.	Was ist ein Virus?	302
b.	Kleine Gattungskunde: Virenarten	304
aa.	Bootviren	304
bb.	Dateiviren	304
cc.	Makroviren	304
dd.	Würmer	305
ee.	Trojanische Pferde	305
ff.	Ransomware	306
gg.	Polymorphe Viren, Stealth-Virus	308
c.	Schäden durch Viren	309
d.	Antivirenprogramme	309
e.	Bitdefender Internet Security	312
f.	Andere Antivirens Scanner	313
g.	Was tun, wenn der PC mit einem Virus infiziert ist?	314
h.	Fazit	315
27.	Sicher ins Internet	316
a.	Cookies	317
b.	»Schweißspur« im Internet	318
c.	Datensammler Suchmaschinen	320
d.	Spuren auf dem Rechner	320
e.	»Spyware« und »Phonehome«	321
f.	Internet Spuren verhindern und löschen	323

g.	Die Alternative: anonymes Surfen?	325
h.	Internetarchiv	328
28.	E-Mails und Newsgroups	330
a.	Gefahren und Abwehr	330
aa.	Ungesicherter Zugang zum Computer und E-Mail-Programm	330
bb.	Ungesichertes Postfach und ungeschützte E-Mails ..	330
cc.	Ungeschütztes Passwort beim Abrufen der E-Mails ..	331
dd.	Falsche E-Mail-Zustellung	331
ee.	Falsche Absenderadresse	331
ff.	Falsche Eingabe bei Weiterleitung einer E-Mail	331
gg.	Fehlende Sicherheitseinstellungen im E-Mail-Programm	332
hh.	Hintertüren und Viren	333
ii.	Fehlende Sicherungen	333
b.	Soziale Netzwerke und Newsgroups – auf ewig gespeichert?	334
c.	Chatten: WhatsApp oder Threema	334
d.	Verschleierte und geschützte E-Mails	337
e.	E-Mail-Sicherheit	339
f.	Telefonieren übers Internet	340
29.	Topsecret! Dateien und E-Mails verschlüsseln	342
a.	Anforderungen des Datenschutzes an die Verschlüsselung von E-Mails mit personenbezogenen Daten	344
b.	Sichere Verschlüsselung?	346
c.	Zwei große Verfahren zur Verschlüsselung	346
d.	Verschlüsselung von Office-Dateien	348
e.	Verschlüsseln von PDF-Dateien	351
f.	Verschlüsseln mit ZIP	353
30.	Verschlüsseln mit dem Betriebssystem	354
a.	Einzelne Dateien und Ordner verschlüsseln mit »Encrypting File System« (EFS)	354
b.	Festplatte mit Windows 10 oder 11 verschlüsseln mit BitLocker	356
c.	USB-Stick verschlüsseln	357
d.	Sicherheitsprobleme	359
e.	Betrieblicher Nachschlüssel	359

Inhaltsverzeichnis

f.	Microsoft und der Bitlocker-Nachschlüssel.....	360
g.	Daten versenden	360
h.	Sicherheit durch die »digitale Signatur«.....	360
31.	Die Verschlüsselungsspezialisten	363
a.	OpenPGP – E-Mails von Betriebs- und Personalräten und Schwerbehindertenvertretungen verschlüsseln.....	363
b.	Kostenlose Verschlüsselung mit »VeraCrypt«.....	372
aa.	Verschlüsseltes Laufwerk oder Containerdatei erstellen.....	374
bb.	Verschlüsselten Container öffnen.....	375
cc.	Verschlüsselten Container schließen	375
c.	Steganos Safe.....	376
32.	Kryptografie verstehen mit »JCrypTool«.....	378
33.	Was Office-Dateien und PDFs so alles verraten.....	381
a.	Kommentare.....	381
b.	Änderungen nachverfolgen	383
c.	Ausgeblendet – der verborgene Text.....	384
d.	Versteckte Infos – die Dokumenteigenschaften	384
e.	Versteckte Informationen in Office-Programmen löschen	387
f.	Dateien richtig löschen	389
g.	Vertrauliche Informationen in PDF-Dokumenten	390
34.	Überwachung im Personalwesen	391
a.	Microsoft 365 – Überwachung und Bewertung	393
b.	Zonar: Ein Beispiel für Überwachung und Bewertung ...	397
35.	Sicherheit bei USB-Sticks	401
a.	Viren und Trojaner bei USB-Sticks.....	402
b.	Verlust und Diebstahl	402
c.	Verschlüsselung von Daten auf USB-Sticks	403
d.	PC-Zugriff per USB-Stick.....	405
e.	Fazit	406
36.	Multifunktionsgeräte als Sicherheitsrisiko.....	409
37.	Datensicherung und Archivierung	412

38. Der sichere Zugang zum Computer der Interessenvertretung	415
a. Sicherheit bei PC-Start	415
b. Sperrbildschirm mit Passwort	417
c. Passwortschutz durch das Zuklappen des Notebooks	418
d. Sicherer PC-Zugang mit Smartcard oder USB-Token	419
e. Sichere Passwörter – das kleine Passwort-ABC	419
39. Daten sicher löschen	425
a. »Wirkliches« Löschen – gar nicht so einfach	426
b. Richtig schreddern im Büro der Interessenvertretung	427
c. Sichere Vernichtung	429
d. Schutzklassen, Sicherheitsstufen unter Materialklassifizierungen	429
e. Richtiges Vorgehen	430
f. Material finden	432
g. Schredder prüfen	432
h. Hardware vernichten	432
i. Vernichtung durch Dritte	433
j. Fazit	433
40. Sicherheit bei Tablet und Notebook	434
a. Diebstahlschutz	434
b. Blickschutz	436
c. Notebookschutz bei kurzzeitiger Abwesenheit	436
d. Integrierte Sicherheit	436
e. WLAN-Hotspots	436
f. Verschlüsselung	437
41. Gegenwart und Ausblick – Datenschutz weltweit und die Gefährdungen für die Demokratie	438
42. Wichtige Internetseiten zum Datenschutz	440
Stichwortverzeichnis	443