

Inhaltsverzeichnis

Vorwort	5
Abkürzungsverzeichnis/Quellenverzeichnis	15
Verzeichnis ausgewählter Literatur	19
Verzeichnis der Checklisten	21
1. Datenschutz in Deutschland	23
a. Gefährdungslage	23
b. Grundlagen des Datenschutzes in Deutschland	27
aa. Datenschutzziele	28
bb. Datenschutzregelungen	29
cc. Aufbau des BDSG	30
dd. Begriffsklärungen	30
ee. Alles, was nicht ausdrücklich erlaubt ist, ist verboten	32
c. Datenvermeidung, Datensparsamkeit und die Datenerhebung	33
aa. Zweckbindung	34
bb. Datenerhebung	36
cc. Vorabkontrolle	36
dd. Übermittlung von Daten	36
ee. Übermittlung ins Ausland	37
d. Auftragsdatenverarbeitung	38
e. Technische und organisatorische Maßnahmen	39
f. Datenschutzpannen	41
g. Rechte der Betroffenen	43
h. Beteiligungsrechte des BR und PR zur Sicherung des Beschäftigtendatenschutzes	45
i. Die Europäische Datenschutz-Grundverordnung	45

Inhaltsverzeichnis

2. Betriebliche und behördliche Datenschutzbeauftragte (bDSB)	49
a. Keine Kontrolle durch den bDSB	49
b. Das Büro der Interessenvertretung, eine datenschutzfreie Zone?	50
3. Der Datenschutzbeauftragte der gesetzlichen Interessenvertretung (DGIV)	52
4. Das Datenschutzsicherheitskonzept der Interessenvertretung	55
5. Angriffe von außen und innen	58
a. Das Firmennetzwerk	59
b. Kontrolle über das Netzwerk	60
c. Sicherheitsrisiko »Sniffer«	62
aa. Das Ausschnüffeln konkret	62
bb. Sniffer abwehren	64
d. WLAN	66
e. Thin Client/Cloud	67
f. Überwachung durch das Betriebssystem	68
g. Zugriff des Systemverwalters auf sensible Daten	68
h. Fazit	69
6. Überwachen und Ausspionieren	71
a. Hintertür-, Fernwartungs- und Kontrollprogramme	71
aa. Die Hintertürprogramme	72
bb. Die wichtigsten Schnüffelfunktionen der Hackertools:	73
cc. Gegenwehr	75
b. Die Fernwartungsprogramme	75
c. Bot-Netze	77
d. Der Chef liest mit – Überwachungsprogramme	79
aa. Big Brother im Betrieb	79
bb. Die Praxis	82
e. Kontrollprogramme entdecken	83
f. Überwachungssoftware auf Handys	84
aa. Handykontrolle total	85
bb. Auswerten der Daten	86
cc. Rechtliche Fragen	86
dd. Was tun?	88
g. Alles rechtens?	89

7. Windows-Datenschutz	91
a. Datenschleuder Windows 10	91
b. Windows-Benutzerkonten	93
8. Die »Brandschutzmauer« zum Internet – persönliche Firewalls	95
a. Die eingebaute Firewall in Windows	96
b. Protokolle einer Firewall	97
c. Fazit	98
9. Seuchengefahr: Computerviren	99
a. Was ist ein Virus?	99
b. Kleine Gattungskunde: Virenarten	102
aa. Bootviren	102
bb. Dateiviren	102
cc. Makroviren	102
dd. Würmer	103
ee. Trojanische Pferde	103
ff. Ransomware	104
gg. Polymorphe Viren, Stealth-Virus	105
c. Schäden durch Viren	106
d. Antivirenprogramme	107
e. Bitdefender Internet Security	109
f. Andere Antivirens Scanner	110
g. Antivirens Scanner testen	111
h. Fazit	112
i. Informationen im Internet	113
10. Sicher ins Internet	114
a. Cookies	115
b. »Schweißspur« im Internet	115
c. Datensammler Suchmaschinen	118
d. Selbsttest Browser, E-Mail, Netzwerk	119
e. Spuren auf dem Rechner	120
f. »Spyware« und »Phonehome«	120
g. Internetspuren verhindern und löschen	122
h. Die Alternative: anonymes Surfen?	122
i. Internetarchiv	126
11. E-Mails und Newsgroups	128
a. Gefahren und Abwehr	128

Inhaltsverzeichnis

aa. Ungesicherter Zugang zum Computer und E-Mail-Programm	128
bb. Ungesichertes Postfach und ungeschützte E-Mails . . .	128
cc. Ungeschütztes Passwort beim Abrufen der E-Mails . . .	129
dd. Falsche E-Mail-Zustellung	129
ee. Falsche Absenderadresse	129
ff. Falsche Eingabe bei Weiterleitung einer E-Mail	129
gg. Fehlende Sicherheitseinstellungen im E-Mail-Programm	130
hh. Hintertüren und Viren	131
ii. Fehlende Sicherungen	131
b. Soziale Netzwerke und Newsgroups – auf ewig gespeichert?	131
c. Chatten: WhatsApp oder Threema	133
d. Verschleierte und geschützte E-Mails	135
aa. Tipps	136
bb. Die geschützte E-Mail – Posteo	137
e. E-Mail-Sicherheit	139
f. Telefonieren übers Internet	139
g. Videokonferenzen	141
12. Topsecret! Dateien und E-Mails verschlüsseln	143
a. Sichere Verschlüsselung?	145
b. Zwei große Verfahren zur Verschlüsselung	145
c. Verschlüsselung von Office-Dateien	147
d. Verschlüsseln von PDF-Dateien	149
13. Verschlüsseln mit dem Betriebssystem	151
a. Festplatte mit Windows 10 verschlüsseln	152
b. USB-Stick verschlüsseln	154
c. Sicherheitsprobleme	155
d. Betrieblicher Nachschlüssel	155
e. Microsoft den Bitlocker-Nachschlüssel entziehen	156
f. Daten versenden	157
g. Sicherheit durch die »digitale Signatur«	158
h. Microsoft Edge, Chrome, Firefox und Outlook	158
i. Tipps für sichere E-Mails	159
14. Die Verschlüsselungsspezialisten	160
a. PGP – der Verschlüsselungsklassiker	160
b. Die PGP-Verschlüsselungsverfahren	161
aa. Der betriebliche Nachschlüssel	162

bb. Gewichtige Gründe für den Nachschlüssel	163
cc. Vereinbarung abschließen, Kontrolle behalten	163
dd. Fazit	164
c. Kostenlose Verschlüsselung mit TrueCrypt oder VeraCrypt	167
d. VeraCrypt im Einsatz	169
aa. Verschlüsseltes Laufwerk oder Containerdatei erstellen	169
bb. Verschlüsselten Container öffnen	170
e. Steganos Privacy Suite	171
aa. Verschlüsseln und verstecken	172
bb. E-Mails verschlüsseln	173
cc. Daten verstecken	174
dd. Spuren per Mausklick vernichten	174
ee. Shredder	175
ff. Passwort-Manager	176
gg. Fazit	176
f. Volksverschlüsselung	177
15. Kryptografie verstehen mit JCrypTool	179
16. Was Office-Dateien und PDFs so alles verraten	182
a. Kommentare	182
b. Änderungen nachverfolgen	184
c. Ausgeblendet – der verborgene Text	184
d. Versteckte Infos – die Dokumenteigenschaften	185
e. Versteckte Infos in Office-Programmen löschen	188
f. Dateien richtig löschen	190
g. Office 365	191
h. Vertrauliche Informationen in PDF-Dokumenten	192
17. Sicherheit bei USB-Sticks	193
a. Viren und Trojaner bei USB-Sticks	194
b. Verlust und Diebstahl	194
c. Verschlüsselung von Daten auf USB-Sticks	195
d. PC-Zugriff per USB-Stick	197
e. Fazit	198
18. Multifunktionsgeräte als Sicherheitsrisiko	201
19. Datensicherung und Archivierung	204

Inhaltsverzeichnis

20. Der sichere Zugang zum Computer der Interessenvertretung	207
a. Sicherheit bei PC-Start	207
b. Energiesparmodus und Bildschirmschoner mit Passwort	209
aa. Energiesparmodus mit Passwort	209
bb. Bildschirmschoner mit Passwort	209
c. Passwortschutz nach dem Zuklappen des Notebooks	210
d. Sicherer Zugang mit Smartcard oder USB-Token	210
e. Sichere Passwörter – das kleine Passwort-ABC	212
21. Daten sicher löschen	215
a. »Wirkliches« Löschen – gar nicht so einfach	216
b. Richtig schreddern im Büro der Interessenvertretung	217
aa. Sichere Vernichtung	218
bb. Schutzklassen, Sicherheitsstufen unter Materialklassifizierungen	219
cc. Richtiges Vorgehen	219
dd. Material finden	221
ee. Schredder prüfen	221
ff. Hardware vernichten	221
gg. Vernichtung durch Dritte	222
c. Fazit	222
22. Sicherheit bei Tablet und Notebook	223
a. Diebstahlschutz	223
b. Seitenblicke	225
c. Notebookschutz bei kurzzeitiger Abwesenheit	225
d. Integrierte Sicherheit	225
e. WLAN-Hotspots	226
f. Verschlüsselung	226
23. Sicherheit bei Smartphones	227
24. Organisationslösungen für das Büro der Interessenvertretung	228
25. Wichtige Internetseiten zum Datenschutz	230
Stichwortverzeichnis	233