Inhalt

Vorwort VII

Abkürzungsverzeichnis XIX

1. Schnelleinstieg – die wichtigsten Fragen im Überblick 1
1.1 Was beinhaltet die EU-Datenschutzreform und wie kann ich mich darauf vorbereiten? 1
1.2 Besteht Meldepflicht der Datenverarbeitung beim Datenverarbeitungsregister? 1
1.3 Ist die Verarbeitung und Übermittlung von Kunden- und Mitarbeiterdaten zulässig? 1
1.4 Entspricht die Zustimmungserklärung zur Datenverarbeitung der aktuellen Judikatur? 2
1.5 Sind die durchgeführten Marketingmaßnahmen zulässig? 2
1.6 Outsourcing: Wurde ein Dienstleistervertrag abgeschlossen? 2
1.7 Ist unser Unternehmensnetzwerk ein genehmigungspflichtiges Informationsverbundsystem? 2
1.8 Wir haben eine Videoüberwachung im Betrieb. Was ist zu tun? 3
1.9 Wie weit darf man seine Mitarbeiter im Betrieb kontrollieren? 3
1.10 Benötigen wir einen betrieblichen Datenschutzbeauftragten? 3
1.11 Was ist zur Daten- und Informationssicherheit zu beachten? 3
1.12 Hilfe, wir haben einen Datenmissbrauchsfall! 3
1.13 Datenschutzrecht interessiert mich nicht? 3

2. Grundbegriffe und Definitionen des Datenschutzgesetzes 5
2.1 Entwicklung und Struktur des Datenschutzrechts 5
2.2 Das künftige EU-Datenschutzrecht 8
2.2.1 Status und Zeithorizont für die Einführung 9
2.2.2 Künftige Strafhöhe 10
2.2.3 Anwendungsbereich der EU-Datenschutzreform 11
2.2.4 Sachlicher und örtlicher Anwendungsbereich 12
2.2.5 Definitionen 13
2.2.6 Grundprinzipien der Datenverarbeitung 13
2.2.7 Rechtmäßigkeit der Verarbeitung 14
2.2.8 Informationspflichten 15
2.2.9 Betroffenenrechte 15
2.2.10 Pflichten des Auftraggebers 17
2.2.11 Gemeinsam verantwortliche Auftraggeber 17
2.2.12 Dienstleister (Auftragsverarbeiter) 17
2.2.13 Dokumentation 18
2.2.14 Datensicherheit und Datenmissbrauch 18

2.2.15 Datenschutz-Folgenabschätzung (Data Protection Impact Assessment) .. 19
2.2.16 Vorabgenehmigung und vorherige Konsultation 20
2.2.17 Datenschutzbeauftragter 20
2.2.18 Verhaltensregelungen 20
2.2.19 Datenübermittlung in Drittstaaten 21
2.2.20 Datenschutzbehörde 21
2.2.21 One-Stop-Shop 22
2.2.22 Beschwerde- und Klagsrechte 23
2.2.23 Schadenersatz 24
2.2.24 Strafen – Details 24
2.2.25 Ausnahmen von der DSGVO 26
2.2.26 Delegierte oder implementierende Rechtsakte 27
2.2.27 Inkrafttreten und Anwendbarkeit 27
2.2.28 Praktische Vorbereitung auf die neue Rechtslage 27
2.2.29 Risikobasierter Compliance-Ansatz 28
2.2.30 Compliance bei neuen und künftigen Projekten 29
2.3 Grundrecht auf Datenschutz und Grundprinzipien 30
2.3.1 Grundrecht auf Datenschutz 30
2.3.2 Grundprinzipien des Datenschutzes 31
2.3.3 Trennung öffentlicher/privater Bereich 34
2.4 Sachlicher Anwendungsbereich des DSG 2000 35
2.4.1. Natürliche und juristische Personen, Personengemeinschaften 35
2.4.2. Automationsunterstützte und manuelle Dateien 35
2.5 Räumlicher Anwendungsbereich des DSG 2000 36
2.6 Definitionen 37
2.6.1 Daten und sensible Daten 37
2.6.1.1 „Normale“ personenbezogene und indirekt personenbezogene Daten 37
2.6.1.2 Sensible Daten 39
2.6.2. Datenanwendung 39
2.6.3 Die drei „Akteure“: Betroffener, Auftraggeber, Dienstleister 41
2.6.4 Informationsverbundsystem 43
2.6.5 Zustimmung 46

3. Meldung beim Datenverarbeitungsregister 47
3.1 Das Datenverarbeitungsregister 47
3.2 Wann besteht Meldepflicht? 50
3.2.1 Grundregel 50
3.2.2 Ausnahmen 51
3.2.3 Ausnahme Standardanwendungen 52
3.2.3.1 Schema der Standardanwendungen 54
3.2.3.2 SA001 Rechnungswesen und Logistik 56
3.2.3.3 SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse 58
3.2.3.4 SA003 Mitgliederverwaltung 59
3.2.3.5 SA007 Verwaltung von Benutzerkennzeichen 61
3.2.3.6 SA022 Kundenbetreuung und Marketing für eigene Zwecke 62
3.2.3.7 SA033 Datenübermittlung im Konzern 63

3.2.4 Vereinfachte Meldung: Musteranwendungen ... 66
3.2.4.1 Musteranwendungen allgemein ... 66
3.2.4.2 Musteranwendung Zutrittskontrolle ... 67
3.3 DVR-Meldungen ... 69
3.3.1 Einsicht in das Datenverarbeitungsregister ... 69
3.3.2 Anmeldung bei DVR-Online ... 70
3.3.2.1 Anmeldung als Vertreter ... 71
3.3.2.2 Anmeldung als berufsmäßiger Parteienvertreter ... 72
3.3.3 Meldung des Auftraggebers ... 72
3.3.3.1 Erstmeldung ... 73
3.3.3.2 Änderungsmeldung ... 74
3.3.3.3 Streichungsmeldung ... 75
3.3.4 Meldung der Datenverarbeitung ... 75
3.3.4.1 Notwendiger Inhalt der Meldung ... 75
3.3.4.2 Erstmeldung ... 78
3.3.4.3 Änderungsmeldung ... 84
3.3.4.4 Streichungsmeldung ... 84
3.3.4.5 Angaben zu den ergriffenen Datensicherheitsmaßnahmen ... 85
3.3.5 Meldung Musteranwendung ... 85
3.4 Ablauf des Meldeverfahrens ... 85
3.4.1 Sofortiger Vollbetrieb ... 85
3.4.2 Ausnahme: Vorabkontrollverfahren ... 86
3.4.3 Prüfungs- und Verbesserungsverfahren ... 86
3.4.4 Eintragung der Meldung ... 89
3.4.4.1 Eintragung ... 89
3.4.4.2 Auflagen ... 89
3.4.4.3 Registerauszug, DVR-Nummer ... 90
3.4.5 Richtigstellung des Registers ... 90
3.5 Führen der DVR-Nummer, Offenlegungspflicht ... 91
3.5.1 Meldepflichtige Datenanwendungen ... 91
3.5.2 Nicht-meldepflichtige Datenanwendungen ... 92

4. Zulässigkeit der Verarbeitung von Daten ... 95
4.1 Einleitung ... 95
4.2 Grundsätze jeder Datenverwendung ... 95
4.2.1 Grundsatz von Treu und Glauben und Rechtmäßigkeit ... 95
4.2.2 Zweckbindungsgrundsatz ... 96
4.2.3 Wesentlichkeitsgrundsatz ... 98
4.2.4 Grundsatz der sachlichen Richtigkeit und Aktualität ... 99
4.2.5 Grundsatz der Datenlöschung ... 100
4.2.6 Zusammenfassung der Grundsätze, Checkliste ... 104
4.3 Zulässigkeit der Verwendung von Daten ... 105
4.3.1 Grundsatz: Verbot der Datenverarbeitung ... 105
4.3.2 Zweck und Inhalt der Datenanwendung ... 106
4.3.3 Gesetzliche Zuständigkeiten/rechtliche Befugnisse ... 107
4.3.4 Schutzwürdige Geheimhaltungsinteressen ... 109
4.3.4.1 Schutzwürdige Geheimhaltungsinteressen bei Verwendung nichtsensibler Daten ... 109

4.3.4.1.1 Ausdrückliche gesetzliche Ermächtigung oder Verpflichtung ... 110
4.3.4.1.2 Zustimmung des Betroffenen ... 110
4.3.4.1.3 Lebenswichtige Interessen ... 111
4.3.4.1.4 Überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten ... 111
4.3.4.1.5 Daten sind veröffentlicht ... 114
4.3.4.1.6 Daten sind nicht personenbezogen ... 114
4.3.4.2 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten ... 116
4.3.5 Erforderliches Ausmaß/gelindestes Mittel ... 121
4.3.6 Prüfschema Zulässigkeit der Datenverarbeitung ... 121

5. Zulässigkeit der Datenübermittlung ... 123
5.1 Übermittlung innerhalb des Unternehmens, Österreichs und der EU ... 123
5.1.1 Arten von Übermittlungen ... 123
5.1.2 Zulässigkeit der Übermittlung ... 126
5.1.2.1 Daten aus zulässiger Datenanwendung ... 126
5.1.2.2 Glaubhaftmachung der rechtlichen Befugnis ... 127
5.1.2.3 Schutzwürdige Geheimhaltungsinteressen ... 129
5.1.3 Prüfschema Zulässigkeit der Datenübermittlung innerhalb des Unternehmens, Österreichs und der EU ... 131
5.2 Übermittlung außerhalb der EU ... 132
5.2.1 Materielle Ausnahmen von der Meldepflicht ... 134
5.2.2 Gleichgestellte Drittstaaten ... 139
5.3 Safe Harbor ... 140
5.4 Standardvertragsklauseln ... 142
5.4.1 Standardvertragsklauseln Verarbeiter ... 144
5.4.1.1 „Gewöhnliche“ Klauseln ... 144
5.4.1.2 „Ungewöhnliche“ Klauseln ... 145
5.4.2 Standardvertragsklauseln der ICC ... 147
5.4.2.1 Standardvertragsklauseln Dienstleister ... 148
5.4.2.1.1 „Gewöhnliche“ Klauseln ... 148
5.4.2.1.2 „Ungewöhnliche“ Klauseln ... 149
5.4.3 Einschaltung von Sub-Dienstleistern ... 150
5.4.4 Zusammenfassung ... 152
5.5 Verbindliche unternehmensinterne Datenschutzregelungen (Binding Corporate Rules) ... 152
5.6 Genehmigung durch die Datenschutzbehörde ... 154
5.6.1 Genehmigungsvoraussetzungen ... 155
5.7 Genehmigungsverfahren ... 156
5.8 Gesamtprüfschema ... 160

6. Problem Zustimmungserklärung ... 165
6.1 Notwendigkeit einer Zustimmung ... 165
6.2 Formulierung der Zustimmungserklärung ... 170
6.2.1 Gesetzliche Bestimmungen ... 171
6.2.2 Rechtsentwicklung ... 173

6.2.2.1 Bundeskanzleramt ... 173
6.2.2.2 Judikatur des OGH ... 174
6.2.2.2.1 Merkur-Entscheidung ... 174
6.2.2.2.2 AGB-der-Banken-Entscheidung I ... 176
6.2.2.2.3 Mobilpoints-Entscheidung ... 177
6.2.2.2.4 AGB-der-Banken-Entscheidung II ... 179
6.2.2.2.5 Kreditvertragsklauseln GE Money Bank ... 181
6.2.2.2.6 Klausel in AGB betreffend Kfz-Finanzierungsleasing ... 185
6.2.2.2.7 AGB Finanzierungsleasing I ... 186
6.2.2.2.8 AGB Finanzierungsleasing II ... 188
6.2.2.2.9 Klauselprüfung Telekommunikationsvertrag ... 189
6.2.2.2.10 ORF-Shop-AGB ... 190
6.3 Lösungsvorschläge ... 193
6.3.1 Zusammenfassung Judikatur ... 193
6.3.2 Musterklausel ... 194
6.3.2.1 Muster korrekte Klausel ... 195
6.3.2.2 Typische Fehler bei der Formulierung von Zustimmungserklärungen ... 196
6.3.2.2.1 Text von Dritten abgeschrieben ... 196
6.3.2.2.2 Zustimmungsklausel zu weit ... 196
6.3.2.2.3 Übermittlung in andere Geschäftsfelder übersehen ... 197
6.3.2.2.4 Datenarten nicht genau beschrieben ... 197
6.3.2.2.5 Zweck nicht genau beschrieben ... 197
6.3.2.2.6 Empfänger nicht genau bezeichnet ... 198
6.3.2.2.7 Hinweis auf Widerruf vergessen ... 200
6.3.2.2.8 Text nicht richtig platziert ... 200
6.3.2.2.9 Sonstige rechtliche „Formalitäten“ nicht beachtet ... 201
6.3.2.3 Zustimmung in Privacy Policies ... 202

7. Outsourcing: Einsatz von Dienstleistern ... 203
7.1 Definition Dienstleister ... 203
7.2 Zulässigkeit der Datenüberlassung an Dienstleister ... 206
7.3 Dienstleisterpflichten, Dienstleistervertrag ... 207
7.3.1. Dienstleisterpflichten ... 208
7.3.2 Cloud Computing ... 212
7.3.2.1 Allgemeines ... 212
7.3.2.2 Wichtige Klauseln ... 213
7.3.2.3 Internationaler Datenverkehr, Subdienstleister ... 214
7.3.2.4 Haftung ... 215
7.3.3 Dienstleistervertrag ... 216
7.4 Prüfschema Datenüberlassung an Dienstleister ... 218

8. Videoüberwachung ... 223
8.1 Definition Videoüberwachung ... 223
8.2 Meldepflichtige Videoüberwachungssysteme ... 226
8.2.1 Ausnahmen von der Meldepflicht ... 228
8.2.2 Verschlüsselung der Daten ... 229
8.2.3 Standardanwendung ... 229

8.3 Sonstige Bestimmungen ... 229
8.3.1 Protokollierungspflicht ... 229
8.3.2 Kennzeichnungspflicht ... 229
8.3.3 Auskunftspflicht ... 230
8.3.4 Übergangsbestimmung ... 232
8.4 Prüfschema Meldung einer Videoüberwachung nach dem DSG ... 233
8.5 Judikatur zu Videoüberwachung ... 234
8.5.1 Judikatur des OGH ... 234
8.5.1.1 Kamera-Attrappen ... 234
8.5.1.2 Überwachung eines fremden Hausdachs ... 234
8.5.1.3 Überwachung des Hausgangs ... 235
8.5.2 Judikatur der früheren Datenschutzkommission (DSK) ... 236
8.5.2.1 Qualitätschecks ... 236
8.5.2.2 Webcam ... 237
8.5.2.3 Videoüberwachung zur Gewinnung von Beweismitteln für einen Zivilrechtsstreit ... 238
8.5.3 Sonstige Judikatur ... 239
8.5.3.1 Umfang der Standardanwendung Videoüberwachung: „Bebautes Privatgrundstück“ ... 239
8.5.3.2 Patientenüberwachung mittels Videoüberwachung ... 240

9. Arbeitnehmerdatenverarbeitung ... 241
9.1 Arbeitnehmerdatenverarbeitung und Arbeitsverfassungsrecht ... 241
9.1.1 Allgemeines ... 241
9.1.2 Mitwirkung und Mitbestimmung der Belegschaft im Unternehmen ... 241
9.1.2.1 Intensität der Mitwirkung ... 241
9.1.2.2 Bereiche der Mitwirkung der Belegschaft ... 242
9.1.3 Betriebsvereinbarungen ... 242
9.1.4. Zustimmungspflichtige Maßnahmen ... 243
9.1.4.1 Personalfragebögen ... 243
9.1.4.2 Kontrollmaßnahmen und technische Systeme ... 245
9.1.4.2.1 Grundlegende Bemerkungen ... 245
9.1.4.2.2 Elektronische Zeiterfassung und Anwesenheitskontrolle ... 247
9.1.4.2.3 Telefonüberwachung ... 247
9.1.4.2.4 Videoüberwachung ... 249
9.1.4.3 Personaldatensysteme und Personalbeurteilungssysteme ... 250
9.1.4.3.1 Personaldatensysteme ... 250
9.1.4.3.2 Personalbeurteilungssysteme ... 253
9.2 Whistleblowing-Hotlines ... 254
9.2.1 Allgemeines ... 254
9.2.2 Richtlinien zur Einführung von „Whistleblowing-Hotlines“ ... 256
9.2.2.1 Auftraggeber der Datenanwendung ... 257
9.2.2.2 Zulässigkeit von Whistleblowing-Hotlines ... 257
9.2.2.3 Betroffene der Datenanwendung ... 258
9.2.2.4 Zulässige Datenarten ... 258
9.2.2.5 Konzerninterne Übermittlung der Meldungen, Beauftragung eines Dienstleisters ... 258

9.2.2.6 Aufbewahrungsdauer der Daten ... 260
9.2.2.7 Abschluss einer Betriebsvereinbarung ... 260
9.3 Kontrolle von E-Mail und Internet am Arbeitsplatz ... 261
9.3.1 Allgemeines ... 261
9.3.2 Kontrolle durch den Arbeitgeber ... 262
9.3.2.1 Berührung der Menschenwürde ... 263
9.3.3 Verbot der Privatnutzung ... 263
9.3.4 Zulässige Privatnutzung ... 265
9.3.5 Drei-Stufen-Modell ... 265
9.3.6 Zusammenfassung ... 267
9.4 IT-Policy, Enduser-Vereinbarung ... 267
9.4.1 Inhalt ... 267
9.4.2 Regelungsvorschlag private E-Mail- und Internetnutzung ... 268
9.5 Social Networks ... 270
9.6 Forensische Untersuchungen ... 271
9.7 Bring your own device – BYOD ... 272

10. Werbemaßnahmen und Datenschutz ... 275
10.1 Bewerbung eigener Kunden ... 275
10.1.1 Allgemeiner rechtlicher Rahmen ... 275
10.1.2 Besondere gesetzliche Bestimmungen für Werbung durch Telekommunikationsmittel ... 276
10.1.2.1 E-Mail-Werbung (Spamming) ... 276
10.1.2.1.1 § 107 TKG ... 276
10.1.2.1.2 Informationspflichten nach dem MedienG und nach dem UWG ... 283
10.1.2.1.3 Informationspflichten nach dem E-Commerce-Gesetz ... 285
10.1.2.1.4 Pflicht zur Offenlegung der Identität des Auftraggebers nach § 25 DSG ... 286
10.1.2.2 Weitere Schnittstellen zwischen TKG und Datenschutz ... 287
10.1.2.2.1 Cookies und Behavioral Advertising ... 287
10.1.2.2.2 Der Rechtsrahmen ... 289
10.1.2.2.3 Die Umsetzung der RL 2009/136/EG in das TKG ... 293
10.1.2.2.4 Logfiles ... 295
10.1.2.2.5 Location Based Services (Standortdaten) ... 296
10.1.3 Einsatz von Dienstleistern ... 298
10.2 Bewerbung fremder Kunden mittels Adressverlagen und Direktmarketingunternehmen ... 298
10.2.1 Begriff Adressverlag und Direktmarketingunternehmen ... 298
10.2.2 Tätigkeit von Adressverlagen und Direktmarketingunternehmen ... 298
10.2.2.1 Datenermittlung ... 298
10.2.2.2 Datenverwendung ... 299
10.2.2.3 Informationspflicht ... 300
10.2.2.4 Auskunfts- und Löschungspflichten, Robinson-Liste ... 300
10.3 Verkauf der eigenen Kundendaten ... 301
10.4 Standesregeln für Adressverlage und Direktmarketingunternehmen ... 302
10.5 Strukturierung von Marketingdatenbanken ... 304

10.6 Big Data ... 305
10.6.1 Definition ... 305
10.6.2 Datenschutzprobleme von Big Data ... 306
10.6.2.1 Pseudonymisierte oder anonymisierte Daten? ... 306
10.6.2.2 Zweckbindung? ... 307
10.6.3 Datenschutzrechtliche Lösungsansätze für Big Data ... 308
10.6.3.1 Zustimmung ... 308
10.6.3.2 Wissenschaftliche Forschung und Statistik ... 308
10.6.3.3 Zusammenfassung der Lösungsansätze ... 310

11. Rechte, Pflichten und Sanktionen nach dem Datenschutzgesetz ... 313
11.1 Pflichten des Auftraggebers und Dienstleisters ... 313
11.1.1 Datensicherheitsmaßnahmen (§ 14 DSG) ... 313
11.1.2 Datengeheimnis (§ 15 DSG) ... 315
11.1.3 Informationspflicht bei Datenmissbrauch (§ 24 Abs 2a DSG) ... 316
11.1.3.1 Pflicht zur Verständigung ... 318
11.1.3.2 Ausnahmen von der Informationspflicht ... 319
11.1.3.3 Keine Pflicht zur Meldung an die Behörde ... 319
11.1.3.4 Sonderregelung im Bereich Telekommunikation ... 320
11.2 Betroffenenrechte ... 321
11.2.1 Auskunftsrecht (§ 26 DSG) ... 322
11.2.2 Richtigstellungs- und Löschungsverpflichtung (§ 27 DSG) ... 326
11.2.3 Widerspruchsrecht (§ 28 DSG) ... 328
11.3 Rechtsschutz ... 329
11.3.1 Kontrollbefugnisse der Datenschutzbehörde ... 330
11.3.2 Beschwerde an die Datenschutzbehörde ... 332
11.3.3 Anrufung der Gerichte ... 335
11.3.4 Schadenersatz ... 336
11.3.4.1 Recht auf Wahrung der Privatsphäre nach § 1328a ABGB ... 338
11.4 Das Rechtsmittelverfahren vor dem Bundesverwaltungsgericht ... 339
11.4.1 Beschwerdegegenstand und die Zuständigkeit ... 340
11.4.2 Beschwerdelegitimation ... 340
11.4.3 Das Verfahren vor dem Bundesverwaltungsgericht ... 341
11.4.4 Das Verfahren für Bescheidbeschwerden ... 341
11.4.5 Das Verfahren für Säumnisbeschwerden ... 342
11.5 Strafen ... 343
11.5.1 Strafen nach dem Strafgesetzbuch ... 343
11.5.2 Strafen nach dem DSG ... 344
11.5.3 Verwaltungsstrafbestimmungen nach dem DSG ... 345
11.6 Sonstige Risiken ... 348
11.6.1 Klage wegen unlauterem Wettbewerb ... 348
11.6.2 Negative Publicity ... 350
11.7 European Privacy Seal (EuroPriSe) ... 351
11.7.1 Einleitung ... 351
11.7.2 Zertifizierungsprozess ... 352
11.7.2.1 Auswahl akkreditierter Experten ... 352
11.7.2.2 Abschluss einer Zertifizierungsvereinbarung ... 352
11.7.2.3 Vereinbarung des „Target of Evaluation“ ... 352

11.7.2.4 Evaluierung durch die Experten ... 352
11.7.2.5 Einreichung des Evaluierungsberichts und Zertifizierung ... 353
11.7.3 Zweck und Nutzen von EuroPriSe ... 353
11.7.4 Kosten der Zertifizierung ... 353

12. Betrieblicher Datenschutzbeauftragter ... 355
12.1 Position und Qualifikation ... 357
12.2 Aufgabenbereich ... 358
12.3 Aus- und Weiterbildung ... 360
12.3.1 Literatur ... 360
12.3.2 Nationale und internationale Seminare und Konferenzen ... 361
12.3.3 Websites und Newsletter mit einschlägigen Informationen ... 361
12.3.4 Behörden, Verbände und Interessenvertretungen ... 362
12.4 Aufbau der Datenschutzorganisation ... 362
12.4.1 „Interner Datenschutzbeirat“ ... 362
12.4.2 Top-Down-Modell ... 362
12.4.3 Bottom-Up-Modell ... 362
12.4.4 Kombinationsmodell ... 363
12.5 Vorschlag für die inhaltliche Arbeit des DSB ... 363
12.5.1 Wichtige Fragen, die immer vom DSB zu stellen sind ... 363
12.5.2 Anlaufstelle für Betroffenenrechte ... 364
12.5.3 Gestaltung von Mitarbeiterschulungen ... 364
12.6 Das erste Jahr als Datenschutzbeauftragter – Aufbau der rechtlichen Prüfung ... 365
12.6.1 Informationen über sämtliche Datenanwendungen beschaffen und auswerten ... 366
12.6.2 Mit beschafften Informationen DVR-Meldepflicht prüfen ... 366
12.6.3 Für DVR-Meldung notwendige Beilagen prüfen ... 367
12.6.4 Für internationalen Datenverkehr notwendige Unterlagen prüfen ... 367
12.6.5 Informationen, die zu Dienstleistern beschafft wurden, aufarbeiten ... 368
12.6.6 Sonstige Prüfung ... 368
12.6.7 Für die Zukunft ... 369
12.7 Datenschutzhandbuch ... 369

13. Datenschutz und Informationssicherheit ... 371
13.1 Grundbegriffe und Ausgangslage ... 371
13.1.1 Begriff der Informationssicherheit ... 371
13.1.2 Datenschutzanforderungen an die Informationssicherheit ... 371
13.1.3 Was sollte der Datenschutzbeauftragte über Informationssicherheit wissen? ... 374
13.2 Grundlagen der Informationssicherheit ... 374
13.2.1 Einführung in das Thema ... 374
13.2.2 Was charakterisiert die Informationssicherheit? ... 377
13.2.3 Informationssicherheits-Standards ... 378
13.2.4 Informationssicherheits-Managementprozess ... 378
13.2.5 Schutzziele der Informationssicherheit ... 380
13.3 Die wichtigsten Säulen der Informationssicherheit ... 380
13.4 Scope (Anwendungsbereich) ... 381

13.5 Informationssicherheit und Datenschutz sind Chefsache ... 382
13.5.1 Sicherheits- und Datenschutzkultur ... 382
13.5.2 Sicherheitsziele – Schutzbedarf ... 382
13.5.3 Informationssicherheitspolitik ... 383
13.5.4 Sicherheitsrichtlinien ... 383
13.5.5 Organisation der Sicherheit – Verantwortlichkeiten ... 384
13.6 Audit – Ist-Analyse – Gap-Analyse ... 384
13.7 Assetmanagement ... 384
13.8 Datenklassifizierung ... 384
13.8.1 Vertraulichkeitsklassifizierung ... 385
13.8.2 Verfügbarkeitsklassifizierung ... 386
13.9 Sicherheitszonen ... 386
13.10 Risikomanagement ... 387
13.10.1 Definitionen ... 387
13.10.2 Sinn eines Risikomanagements ... 387
13.10.3 Problematik beim Risikomanagement ... 388
13.10.4 Risikomanagement aus Datenschutzsicht ... 389
13.10.5 Risikomanagement: Praktischer Lösungsansatz in sieben Schritten ... 390
13.10.6 Resümee zum Risikomanagement ... 395
13.11 Notfallsmanagement ... 396
13.12 Informationssicherheitshandbuch – Awareness – Compliance ... 396
13.12.1 Informationssicherheitshandbuch ... 396
13.12.2 Awareness ... 400
13.12.3 Compliance ... 401
13.13 Zusammenarbeit Datenschutzbeauftragter – Informationssicherheits-Manager ... 401
13.14 Technik und Organisation ... 401
13.15 Nichts vergessen ... 405
13.16 Ausblick ... 405

14. Anhang – Standardanwendungen ... 407
14.1 SA001 Rechnungswesen und Logistik ... 407
14.2 SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse ... 412
14.3 SA003 Mitgliederverwaltung ... 423
14.4 SA007 Verwaltung von Benutzerkennzeichen ... 425
14.5 SA022 Kundenbetreuung und Marketing für eigene Zwecke ... 426
14.6 SA032 Videoüberwachung ... 428
14.7 SA033 Datenübermittlung im Konzern ... 442
14.8 SA036 Hinweisgebersysteme gemäß § 99g BWG ... 447

Literatur ... 451

Stichwortverzeichnis ... 465