

# Inhaltsverzeichnis

Vorwort .....	VII
Autorenverzeichnis .....	XXVII
Abkürzungsverzeichnis .....	XXIX
Literaturverzeichnis .....	XLI

## 1. Kapitel

### Schnelleinstieg – To-Dos und die wichtigsten Fragen im Überblick

*Rainer Knyrim*

I. Wie ist der aktuelle Entwicklungsstand des Datenschutzrechts in der EU und in Österreich? .....	1
II. Betrifft uns das Datenschutzrecht und welche Rolle haben wir? .....	1
III. Was muss ein Verarbeitungsverzeichnis enthalten? .....	2
IV. Wann ist die Verarbeitung von Kunden-, Lieferanten- und Mitarbeiterdaten zulässig? .....	2
V. Wie formuliert man eine Einwilligungserklärung zur Datenverarbeitung richtig? .....	2
VI. Unter welchen Voraussetzungen dürfen personenbezogene Daten in Drittstaaten übermittelt werden? .....	2
VII. Welche Informationspflichten treffen uns und wie reagieren wir auf Betroffenenanfragen? .....	3
VIII. Liegt eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vor und was ist dann zu tun? .....	3
IX. Was ist zur Daten- und Informationssicherheit zu beachten? .....	3
X. Hilfe! – Data Breach! Was ist zu tun? .....	4
XI. Wann und wie müssen wir eine Datenschutz-Folgenabschätzung machen und die Datenschutzbehörde konsultieren? .....	4
XII. Benötigen wir einen betrieblichen Datenschutzbeauftragten und wie und mit welchen Aufgaben ist dieser zu installieren? .....	4
XIII. Sind für uns Verhaltensregeln oder Zertifizierungen sinnvoll und wie gelangt man zu diesen? .....	5
XIV. Wir machen Fotoaufnahmen und betreiben eine Videoüberwachung. Dürfen wir das? Was ist zu tun? .....	5
XV. Wie weit dürfen wir unsere Mitarbeiter kontrollieren? .....	5
XVI. Sind unsere durchgeführten Marketingmaßnahmen zulässig? .....	6

XVII. Welche Erleichterungen gibt es für die Datenverarbeitung zu Archiv-, Forschungs- oder statistischen Zwecken? .....	6
XVIII. Datenschutzrecht ist mir egal! Was soll schon passieren? .....	6
XIX. Wie setzen wir unsere Datenschutz-Projekte in der Praxis um? Was für typische Fehler werden gemacht und wie können wir diese vermeiden? .....	7

## 2. Kapitel

### Entwicklung und Struktur des Datenschutzrechts

*Rainer Knyrim*

I. Vom DSG 1978 zum DSG 2000 .....	9
II. DSGVO .....	11
III. Datenschutz-Anpassungsgesetz 2018 – neues DSG .....	12
IV. Datenschutz-Deregulierungs-Gesetz 2018 .....	13
V. Kompetenzentflechtungspaket .....	15
VI. Materiengesetze zum DSG .....	15
VII. Verordnungen der Datenschutzbehörde zum DSG .....	16
VIII. ePrivacy-Verordnung .....	16
IX. Leitlinien des Europäischen Datenschutzausschusses .....	17

## 3. Kapitel

### Grundbegriffe und Definitionen

*Viktoria Haidinger*

I. Grundrecht auf Datenschutz .....	19
II. Grundprinzipien des Datenschutzes .....	20
III. Persönlicher und sachlicher Anwendungsbereich .....	24
A. Wer ist geschützt? .....	25
B. Personenbezogene Daten .....	26
1. Informationen .....	26
2. Identifizierbarkeit, Datentypen .....	27
a) Pseudonyme Daten .....	27
b) Anonyme Daten .....	29
c) Besonders geschützte Daten .....	29
C. Automationsunterstützte und manuelle Dateien .....	32
IV. Räumlicher Anwendungsbereich .....	33
V. Datenverarbeitung .....	35
VI. Die „Akteure“ des Datenschutzrechts .....	35
VII. Einwilligung .....	39

## 4. Kapitel

### Verarbeitungsverzeichnis

*Ursula Illibauer*

I. Inhalt des Verarbeitungsverzeichnisses eines Verantwortlichen .....	42
II. Inhalt des Verarbeitungsverzeichnisses eines Auftragsverarbeiters .....	43
III. Form .....	44
IV. Ausnahme .....	47

**5. Kapitel  
Zulässigkeit der Verarbeitung von Daten**

*Viktoria Haidinger*

I. Einleitung .....	49
II. Grundsätze jeder Datenverarbeitung .....	49
A. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz .....	49
B. Zweckbindung .....	51
C. Datenminimierung .....	56
D. Richtigkeit .....	59
E. Speicherbegrenzung .....	60
F. Integrität und Vertraulichkeit .....	64
G. Rechenschaftspflicht .....	64
H. Zusammenfassung der Grundsätze, Checkliste .....	65
III. Rechtmäßigkeit der Datenverarbeitung .....	66
A. Grundsatz: Verbot der Datenverarbeitung .....	67
B. Zweck und Inhalt der Datenverarbeitung .....	68
C. Gesetzliche Zuständigkeiten/rechtliche Befugnisse .....	69
D. Rechtmäßigkeitsgrundlagen .....	71
1. Kanon der Rechtmäßigkeitsgrundlagen .....	71
a) Einwilligung .....	72
b) Vertragserfüllung .....	72
c) Rechtliche Grundlage .....	74
d) Lebenswichtige Interessen .....	74
e) Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt .....	74
f) Berechtigte Interessen .....	75
g) Anonyme Daten .....	78
2. Anwendung auf normale Daten .....	78
3. Anwendung auf sensible Daten .....	78
a) Einwilligung .....	79
b) Vertragserfüllung .....	79
c) Rechtliche Grundlage .....	80
d) Lebenswichtige Interessen .....	81
e) Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt .....	81
f) Berechtigte Interessen .....	81
4. Anwendung auf strafrechtlich relevante Daten .....	82
5. Zweckändernde Weiterverarbeitung .....	82
6. Verhältnismäßigkeit iES .....	82
E. Prüfschema Zulässigkeit der Datenverarbeitung .....	82
IV. Besonderheiten der Datenübermittlung .....	84
A. Daten aus zulässiger Datenverarbeitung .....	84
B. Glaubhaftmachung der rechtlichen Befugnis .....	85
C. Rechtmäßigkeit der „neuen“ Datenverarbeitung .....	87

**6. Kapitel**  
**Problem Einwilligungserklärung**

*Katja WYROBEK*

I. Notwendigkeit einer Einwilligung .....	89
A. Sonderfall: Dienste der Informationsgesellschaft .....	90
B. Sonderfall: Internationaler Datenverkehr .....	93
C. Sonderfall automatisierte Entscheidungsfindung (einschließlich Profiling) .....	93
D. Zusammenfassung .....	93
E. Umgang mit bestehenden Einwilligungen .....	94
F. Rechtsfolgen .....	95
II. Notwendige Elemente einer Einwilligungserklärung .....	95
A. Gesetzliche Bestimmungen .....	95
1. Freiwilligkeit .....	95
2. Bestimmtheit .....	97
3. Informiertheit .....	98
4. Eindeutige Handlung .....	99
a) Konkludente Einwilligung .....	100
b) Sonderfall ausdrückliche Einwilligung .....	100
B. Bedingungen für die Einwilligung .....	101
1. Nachweisbarkeit .....	101
2. Transparenz .....	101
3. Widerrufbarkeit .....	102
4. Koppelungsverbot .....	102
III. Judikatur .....	104
A. Judikatur der Datenschutzbehörde .....	104
1. Dienstleistungs-Club .....	104
2. Allergie-Tagesklinik .....	106
3. DerStandard.at Cookie-Wall .....	108
4. Veranstaltungsakkreditierung des Bundesministeriums .....	110
5. Action-Cam der Sommerrodelbahn .....	111
B. Judikatur des Bundesverwaltungsgerichts .....	112
1. Übergabe einer Patientenkartei .....	112
2. Einwilligungsfähigkeit der Nutzung von GPS-Daten von Mitarbeiterfahrzeugen .....	113
C. Oberster Gerichtshof .....	113
1. Merkur-Entscheidung .....	114
2. AGB-der-Banken-Entscheidung I .....	115
3. Mobilpoints-Entscheidung .....	116
4. AGB-der-Banken-Entscheidung II .....	118
5. Kreditvertragsklauseln GE Money Bank .....	120
6. Klausel in AGB betreffend Kfz-Finanzierungsleasing .....	124
7. AGB Finanzierungsleasing I .....	125
8. Klauselprüfung Telekommunikationsvertrag .....	127
9. ORF-Shop-AGB .....	128
10. Klauselprüfung Simpli-TV .....	130

11. Klauselprüfung Pay-TV .....	132
12. Hotelgutschein-Vermittler/Midnight Deal .....	134
D. Allgemeine Grundsätze .....	135
E. Internationale Erkenntnisse .....	137
1. Einwilligung im Beschäftigungskontext .....	137
2. Gesichtserkennungssoftware in Schwedischer Schule .....	138
3. Mangelhafter Cookie-Einsatz einer Fluglinie .....	138
IV. Musterklausel .....	139
A. Musterklausel .....	139
B. Beispiel einer Einwilligungserklärung .....	139
V. Typische Fehler bei der Formulierung von Einwilligungserklärungen .....	141
A. Eine Einwilligung ist nicht nötig .....	141
B. Widerruf vergessen .....	141
C. Text abgeschrieben .....	141
D. Übermittlungsempfänger nicht angegeben .....	142
E. Datenarten nicht beschrieben .....	142
F. Zwecke nicht ausreichend beschrieben .....	142
G. Text falsch platziert .....	142
H. Koppelungsverbot missachtet .....	142
I. Mangelnde Freiwilligkeit .....	143
J. Cookies .....	143
VI. Einwilligung in Privacy Policies .....	144

## 7. Kapitel Internationaler Datenverkehr

*Rainer Knyrim*

I. Grundsätze für die Übermittlung außerhalb der EU .....	145
A. Grundprinzip .....	145
B. Anwendbarkeit der Regeln .....	146
C. Übermittlungsempfänger .....	147
D. Weiterleitungsketten .....	148
E. Prüfschema .....	149
II. Gleichgestellte Drittstaaten und Privacy Shield .....	152
A. Liste der gleichgestellten Drittstaaten .....	152
B. EU-US Privacy Shield .....	154
1. Vorgänger Safe Harbor .....	154
2. Privacy Shield als Nachfolger .....	155
3. Voraussetzungen für Datentransfers unter dem Privacy-Shield-Übereinkommen .....	156
4. Die ungewisse Zukunft des Privacy-Shield-Übereinkommens .....	159
III. Datenübermittlung vorbehaltlich geeigneter Garantien .....	160
A. Rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen .....	163
B. Verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“) .....	163
1. Entwicklung und Praxisbedeutung .....	163
2. Inhalt und Genehmigung von Binding Corporate Rules .....	164

C. Neue Standarddatenschutzklauseln der Kommission .....	168
D. Weitergeltung der bisherigen Standardvertragsklauseln .....	170
1. Standardvertragsklauseln Verantwortliche .....	172
a) „Gewöhnliche“ Klauseln .....	172
(1) Definitionen, Inhalt der Übermittlung .....	172
(2) Pflichten .....	173
(3) Weitere „gewöhnliche“ Klauseln .....	173
b) „Ungewöhnliche“ Klauseln .....	174
(1) Drittbegünstigtenklausel .....	174
(2) Haftungsklauseln .....	174
(3) Anwendbares Recht und Gerichtsstand .....	175
2. Standardvertragsklauseln der ICC .....	175
3. Standardvertragsklauseln für Auftragsverarbeiter .....	176
a) „Gewöhnliche“ Klauseln .....	177
b) „Ungewöhnliche“ Klauseln .....	178
4. Hinzuziehung von Sub-Dienstleistern .....	179
E. Von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln .....	180
F. Genehmigte Verhaltensregeln .....	181
G. Genehmigter Zertifizierungsmechanismus .....	181
H. Von der Datenschutzbehörde genehmigte Vertragsklauseln .....	182
I. Behördlich genehmigte Bestimmungen in Verwaltungsvereinbarungen .....	185
IV. Datenübermittlung aufgrund von Urteilen und Verwaltungsentscheidungen aus Drittländern oder internationalen Übereinkommen .....	186
V. Datentransfer auf Basis „besonderer Ausnahmen“ .....	187
A. „Gelegentlich“ und „nicht wiederholend“ .....	188
B. Ausnahmenkatalog .....	188
1. Einwilligung .....	188
2. Vertragsanbahnung oder -erfüllung .....	189
3. Wichtige Gründe des öffentlichen Interesses .....	192
4. Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen .....	193
5. Schutz lebenswichtiger Interessen .....	194
6. Übermittlung aus einem Register .....	195
7. Einzelfallabwägung .....	195

## 8. Kapitel Informationspflichten und Betroffenenrechte

*Viktoria Haidinger/Ursula Illibauer*

I. Einleitung .....	199
II. Grundsätze und Verfahren .....	200
A. Formulierung .....	201
B. Form .....	203
1. Informationspflichten („Datenschutzerklärung“) .....	205
2. Mitteilungen und Maßnahmen im Rahmen von Betroffenenrechten .....	208
C. Erleichterungsgrundsatz .....	208
D. Identität .....	209
E. Fristen .....	211

III. Betroffenenrechte .....	213
A. Für alle Rechte geltende Bestimmungen .....	215
1. Gemeinsame Bestimmungen .....	215
2. Unternehmensinterner Prozess .....	218
B. Recht auf Auskunft (Art 15 DSGVO) .....	218
1. Welche Voraussetzungen hat das Auskunftsrecht? .....	220
2. Was hat die Auskunft zu umfassen? .....	220
a) Konkret verarbeitete Daten (Abs 1) .....	220
b) Recht auf Datenkopie (Abs 3) .....	221
c) Zusatzinformationen (Abs 1 lit a-h, Abs 2) .....	221
3. Kann die Auskunft verweigert werden? .....	222
C. Rechte auf Berichtigung (Art 16 DSGVO), Löschung (Art 17 DSGVO) und Einschränkung (Art 18 DSGVO) .....	224
1. Welche Voraussetzungen haben diese Rechte? .....	226
a) Berichtigung (Art 16 DSGVO) .....	226
b) Löschung (Art 17 Abs 1 DSGVO) .....	227
c) Einschränkung (Art 18 Abs 1 DSGVO) .....	228
2. Wie ist der Antrag umzusetzen? .....	228
3. Kann der Antrag abgelehnt werden? .....	229
4. Spezielle Mitteilungspflichten .....	231
D. Recht auf Datenübertragbarkeit (Art 20 DSGVO) .....	232
1. Welche Voraussetzungen hat das Recht auf Datenübertragbarkeit? .....	232
2. Wie ist der Antrag umzusetzen? .....	233
3. Kann der Antrag abgelehnt werden? .....	234
E. Widerspruchsrecht (Art 21 DSGVO) .....	234
1. Welche Voraussetzungen hat der Widerspruch? .....	235
2. Wie ist der Antrag umzusetzen? .....	236
3. Kann der Antrag abgelehnt werden? .....	236
F. Recht auf Intervention bei einer automatisierten Entscheidung im Einzelfall (Art 22 DSGVO) .....	237
1. Voraussetzungen für das Verarbeitungsverbot .....	238
2. Ausnahmen vom Verarbeitungsverbot .....	240
3. Angemessene Schutzmaßnahmen, Recht auf Intervention .....	241
IV. Informationspflichten .....	242
A. Datenerhebung erfolgt bei der betroffenen Person .....	244
B. Datenerhebung erfolgt bei Dritten .....	250

## **9. Kapitel Outsourcing und Kooperationen**

*Ursula Illibauer*

I. Definition Auftragsverarbeiter .....	255
II. Zulässigkeit der Datenweitergabe an Auftragsverarbeiter .....	259
III. Auftragsverarbeiterpflichten, Auftragsverarbeitervertrag .....	260
A. Auftragsverarbeiterpflichten .....	260
1. Hinreichende Garantien des Auftragsverarbeiters .....	261
2. Haftung/Warnpflicht .....	261

3. Sub-Auftragsverarbeiter .....	262
B. Auftragsverarbeitervertrag .....	263
1. Form des Vertrages .....	264
2. Weisungsgebundenheit .....	265
3. Mitarbeiterbelehrung .....	265
4. Datensicherheitsmaßnahmen .....	267
5. Sub-Auftragsverarbeiter .....	267
6. Unterstützungspflicht .....	267
7. Beendigung des Auftragsverarbeiterverhältnisses .....	268
8. Überprüfungspflicht .....	269
9. Sonstige Inhalte .....	269
C. Cloud-Computing .....	270
1. Allgemeines .....	270
2. Wichtige Klauseln .....	271
a) Rechts- und Gerichtsstandswahl .....	271
b) Service Level Agreement .....	271
c) Art 28 DSGVO .....	271
d) Beendigung des Vertragsverhältnisses .....	271
3. Internationaler Datenverkehr, Sub-Auftragsverarbeiter .....	271
IV. Gemeinsam Verantwortliche .....	272

## 10. Kapitel DSGVO und Informationssicherheit

*Hans-Jürgen Pollirer*

I. Einleitung .....	277
II. Der risikobasierte Ansatz in der DSGVO .....	279
A. Exkurs zum Thema „Stand der Technik“ .....	280
III. Ziele der Informationssicherheit .....	283
IV. Das Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 für größere Organisationen bzw Organisationen, die in kritischen Bereichen tätig sind .....	285
V. Planung, Einführung, Überprüfung und Verbesserung des ISMS .....	287
A. Phase 1 (Plan) .....	287
B. Phase 2 (Do) .....	290
1. Exkurs: Auswahl von technischen und organisatorischen Maßnahmen nach der ZAWAS-Methode .....	294
2. Exkurs zum Datengeheimnis gem § 6 DS-G .....	297
C. Phase 3 (Check) .....	300
D. Phase 4 (Act) .....	300
E. Exkurs: Das Informationssicherheits-Managementsystem (ISMS) für kleine und mittlere Organisationen .....	300
VI. Die Zertifizierung des ISMS nach ISO/IEC 27001 .....	302
VII. Datenschutz durch Technikgestaltung (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default) gem Art 25 DSGVO .....	303



**11. Kapitel  
Data Breach**

*Andreas Zavadil*

I. Allgemeines .....	309
II. Begriffsdefinition: „Data Breach“ .....	310
III. Meldepflicht an die Aufsichtsbehörde (Art 33) .....	312
A. Frist zur Meldung .....	313
1. Bekanntwerden des Vorfalls und Regelfrist .....	313
2. Überschreiten der Regelfrist .....	314
3. Fristberechnung .....	315
B. Inhalt der Meldung .....	316
C. Schrittweise Meldung .....	318
D. Verfahrensrechtliche Aspekte .....	319
E. Protokollierungspflicht .....	321
IV. Benachrichtigung der betroffenen Personen (Art 34) .....	322
A. Inhalt der Benachrichtigung .....	322
B. Anforderungen an die Kommunikation .....	323
C. Absehen von der individuellen Benachrichtigung .....	324
1. Zuvor getroffene Maßnahmen .....	324
2. Nachträglich getroffene Maßnahmen .....	325
3. Unverhältnismäßig hoher Aufwand .....	326
D. Die Benachrichtigung als durchsetzbares Recht .....	326
V. Risikobewertung .....	327
A. Risikoabwägung der Art-29-Datenschutzgruppe .....	327
B. Berechnungsmethodik der ENISA .....	329
1. Der falsche Rechnungsempfänger .....	331
2. Die offengelegte Kirchenbeitragsvorschrift .....	331
3. Das zerstörte Daten-Backup .....	332

**12. Kapitel  
Datenschutz-Folgenabschätzung, Konsultation**

*Rainer Knyrim*

I. Datenschutz-Folgenabschätzung .....	333
A. Allgemeines .....	333
B. Auslöser einer Datenschutz-Folgenabschätzung .....	335
1. Form der Verarbeitung .....	335
2. Hohes Risiko .....	336
C. Prüfschema Notwendigkeit einer Datenschutz-Folgenabschätzung .....	337
1. Allgemeine Erläuterungen zur Prüfsystematik .....	337
2. Prüfschema in Einzelschritten .....	338
a) Gibt es eine Datenschutz-Folgenabschätzung des Gesetzgebers? .....	338
b) Wurde eine vorabkontrollpflichtige DVR-Meldung durchgeführt? .....	339
c) War die Datenanwendung vor der DSGVO meldefrei? .....	341
d) Whitelist .....	342
e) Blacklist .....	349

f) Art 35 Abs 1 und 3 .....	354
g) Die neun Kriterien der Art-29-Datenschutzgruppe .....	356
3. Gesamtprüfschema .....	359
D. Durchführung der Datenschutz-Folgenabschätzung .....	367
1. Allgemeines .....	367
2. Erstellung der Datenschutz-Folgenabschätzung .....	367
3. Dokumentation und regelmäßige Überprüfung .....	372
II. Vorherige Konsultation der Datenschutzbehörde .....	373
A. Auslöser der Konsultationsverpflichtung .....	373
B. Konsultationsantrag .....	374
C. Konsultationsverfahren .....	374

## **13. Kapitel Datenschutzbeauftragte**

*Michael Löffler*

I. Einleitung .....	377
II. Benennungspflichten .....	377
A. Wer muss Datenschutzbeauftragte benennen? .....	377
1. Benennungspflicht für Behörden/öffentliche Stellen .....	378
2. Benennungspflicht bei bestimmter Kerntätigkeit .....	379
a) Regelmäßige, systematische Überwachung als Kerntätigkeit .....	380
b) Umfangreiche Überwachung/umfangreiche Verarbeitung „sensibler“ Daten als Kerntätigkeit .....	380
B. Gemeinsame Datenschutzbeauftragte für mehrere Verantwortliche/ Auftragsverarbeiter .....	381
C. Nationale Benennungspflichten – regelmäßige Evaluation .....	382
D. Freiwillige Benennung von DSBA .....	383
III. Anforderungen an DSBA .....	384
IV. Interne oder externe DSBA? .....	388
V. Formale Benennungsvoraussetzungen .....	389
VI. Mindest- bzw Höchstbenennungsdauer .....	390
VII. Rolle von DSBA .....	391
A. Frühzeitige Einbindung von DSBA .....	391
B. Welche Ressourcen brauchen DSBA? .....	392
1. Zeit, Räumlichkeiten, interne/externe Unterstützung .....	392
2. Mitarbeiter .....	393
3. Zugang zu personenbezogenen Daten .....	393
4. Fort- und Weiterbildungsmöglichkeiten .....	395
C. Weisungsfreiheit und „Kündigungsschutz“ von DSBA .....	395
D. Berichtspflichten von DSBA .....	396
E. Verhältnis von DSBA zu betroffenen Personen .....	397
F. Geheimhaltungspflicht von DSBA .....	399
VIII. Welche (Mindest-)Aufgaben haben DSBA? .....	400
A. Schaffung eines Überblicks über Verarbeitungstätigkeiten .....	401
B. Spezifische Beratungs- und Prüfaufgaben .....	402

C. Sensibilisierungs- bzw Schulungsmaßnahmen .....	403
D. Aufgaben von DSBA bei DSFA .....	404
E. Zusammenarbeit mit der Aufsichtsbehörde .....	404
IX. Sonstige Aufgaben von DSBA .....	405
X. Interessenkonflikte von DSBA .....	406
XI. Haftung von DSBA .....	407
XII. Checkliste DSBA .....	407

## **14. Kapitel Verhaltensregeln und Zertifizierung**

*Rainer Knyrim/Maximilian Kröpfl*

I. Zweck von Verhaltensregeln und Zertifizierungen .....	409
II. Mehrwert und Anwendungsfälle von Verhaltensregeln und Zertifizierungen .....	413
A. Normative Vorteile .....	414
1. Nachweispflicht .....	414
2. Heranziehen von Auftragsverarbeitern .....	415
3. Sicherheit der Verarbeitung .....	415
4. Datenschutz-Folgenabschätzung .....	416
5. Geeignete Garantie für den internationalen Datentransfer .....	417
6. Milderungsgrund im Verwaltungsstrafverfahren .....	417
B. Betriebliche Vorteile .....	417
1. Risikomanagement des Verantwortlichen .....	418
2. Wettbewerbsvorteil .....	418
3. Öffentliche Ausschreibungen .....	419
III. Auflegen und Implementieren von Verhaltensregeln .....	419
A. Vorüberlegungen .....	419
B. Inhaltliche Gestaltung von Verhaltensregeln .....	420
1. Fakultativer Inhalt von Verhaltensregeln .....	420
2. Obligatorischer Inhalt von Verhaltensregeln .....	421
C. Genehmigung der Verhaltensregeln durch die Aufsichtsbehörde .....	423
1. Implementierung .....	423
IV. Zertifizierung von Verantwortlichen und Auftragsverarbeitern .....	424
A. Zertifizierungsantrag und Antragsbewertung .....	424
B. Evaluierung und Zertifizierung .....	425
C. Wirkungsrelevante Änderungen .....	426
V. Überwachungs- und Zertifizierungsstellen .....	426
A. Eignung als Konformitätsbewertungsstellen .....	426
B. Unabhängigkeit und Interessenkonflikte .....	428
C. Fachwissen .....	429
D. Verfahren zur Konformitätsbewertung, Überwachung und Prüfung .....	430
E. Beschwerdemanagement .....	430
F. Berichtspflicht an die Datenschutzbehörde .....	431
VI. Streitigkeiten mit der Konformitätsbewertungsstelle .....	431
VII. Widerruf und Sanktionen .....	432
A. Widerruf der Genehmigung .....	432
B. Sanktionen .....	433

**15. Kapitel  
Bildverarbeitung (Videoüberwachung)**

*Michael Löffler*

I. Sonderstellung von Bildverarbeitungen .....	435
II. Was sind Bildaufnahmen? .....	436
A. Bilddaten sind nicht grundsätzlich besondere Kategorien von Daten .....	437
III. Wann sind Bildverarbeitungen zulässig? .....	438
A. Einhaltung allgemeiner datenschutzrechtlicher Grundsätze .....	438
B. Rechtmäßigkeit von Bildverarbeitungen .....	438
1. Einwilligung als Rechtsgrundlage .....	439
2. Berechtigte Interessen als Rechtsgrundlage .....	439
a) Erfassung unvermeidbarer öffentlicher Verkehrsflächen .....	440
b) Zeitliche Dimension von Videoüberwachung .....	441
c) (Un)Zulässigkeit von „Dash-Cams“ .....	441
d) Zulässigkeit von Drohnen? .....	443
e) Fotos von Mitarbeitern auf Unternehmenswebsites .....	445
f) Rechtmäßigkeit von Veranstaltungsfotografie .....	446
IV. Übermittlung/Veröffentlichung von Bildaufnahmen .....	446
V. Unzulässige Bildverarbeitungen .....	447
A. Erfassung des höchstpersönlichen Lebensbereichs .....	447
B. Automationsunterstützter Abgleich von Bildaufnahmen/ Erstellung von Persönlichkeitsprofilen .....	448
C. Kontrolle von Arbeitnehmern .....	449
D. Auswertung von Bildaufnahmen anhand besonderer Kategorien personenbezogener Daten .....	451
E. Gewinnung von Beweismitteln in Rechtsstreitigkeiten .....	451
F. Allgemeiner Persönlichkeitsschutz .....	452
1. Kameraattrappen .....	452
2. Unzulässiges Fotografieren .....	453
VI. Datenschutz-Folgenabschätzungen .....	454
VII. Datensicherheitsvorschriften .....	455
A. Protokollierungspflicht .....	455
VIII. Löschungspflicht .....	456
IX. Informationspflicht .....	457
A. Kennzeichnung von Videoüberwachungen .....	458
X. Betroffenenrechte .....	459
A. Auskunftsrecht .....	459
B. Löschungs- bzw Widerspruchsrecht .....	462
XI. Strafbestimmungen .....	463
XII. Checkliste Bildverarbeitungen (Videoüberwachungen) .....	463

**16. Kapitel  
Arbeitnehmerdatenverarbeitung**

*Viktoria Haidinger*

I. Arbeitnehmerdatenverarbeitung und Arbeitsverfassungsrecht .....	465
A. Allgemeines .....	465
B. Rechtmäßigkeitsgrundlagen im Arbeitsverhältnis – Überblick .....	465

C. Mitwirkung und Mitbestimmung der Belegschaft im Unternehmen im Überblick .....	466
1. Intensität der Mitwirkung .....	466
2. Bereiche der Mitwirkung der Belegschaft .....	467
D. Betriebsvereinbarungen .....	468
E. Zustimmungspflichtige Maßnahmen .....	469
1. Disponible Betriebsvereinbarungen .....	469
a) Personalfragebögen .....	469
b) Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer .....	471
2. Erzwingbare Betriebsvereinbarungen .....	473
a) Personaldatensysteme .....	473
(1) Abgrenzung § 96 und § 96a ArbVG – Wandlungsthese des OGH .....	476
b) Personalbeurteilungssysteme .....	478
II. Anwendungsfälle .....	480
A. Elektronische Zeiterfassung und Anwesenheitskontrolle .....	480
B. Bildverarbeitung .....	481
C. Die Kontrolle der Kommunikation des Arbeitnehmers .....	484
1. Allgemeines .....	484
2. Kontrolle durch den Arbeitgeber .....	486
3. Verbot der Privatnutzung .....	486
4. Zulässige Privatnutzung .....	489
5. Drei-Stufen-Modell .....	490
a) Stufe 1: Maschinelle Überwachung zur Gewährleistung der Systemfunktionalität .....	490
b) Stufe 2: Signifikante Abweichungen von der „normalen“ IT-Nutzung .....	490
c) Stufe 3: Zugriff auf Kommunikationsdaten bei Verdacht auf (Vertrags-)Rechtsverletzung .....	491
d) Verhältnismäßigkeit .....	491
6. Zusammenfassung .....	491
7. IT-Policy, Enduser-Vereinbarung .....	492
a) Inhalt .....	492
b) Regelungsvorschlag private E-Mail- und Internetnutzung .....	493
D. Bring your own device – BYOD .....	495
E. Die Verarbeitung von Standortdaten und Industrie 4.0 .....	497
1. Allgemeines .....	497
2. Fallkonstellationen .....	499
a) Erfüllung der Rechte und Pflichten aus dem Arbeitsvertrag .....	499
b) Arbeitsrechtliche Kontrolle .....	500
c) Arbeitnehmerschutz .....	500
d) Sonstige berechnigte Interessen .....	500
e) Gesetzliche Verpflichtung .....	501
3. Verhältnismäßigkeit .....	502
F. Forensische Untersuchungen .....	503
G. Whistleblowing-Hotlines .....	505
1. Allgemeines .....	505
2. Richtlinien zur Einführung von „Whistleblowing-Hotlines“ .....	507

a) Verantwortlicher der Datenverarbeitung .....	507
b) Zulässigkeit von Whistleblowing-Hotlines .....	507
c) Betroffene der Datenverarbeitung .....	508
d) Zulässige Datenarten .....	508
e) Konzerninterne Übermittlung der Meldungen, Beauftragung eines Auftragsverarbeiters .....	509
f) Aufbewahrungsdauer der Daten .....	509
g) Abschluss einer Betriebsvereinbarung .....	510
H. Die Corona Krise 2020 .....	510
1. Datenverarbeitungen im Betrieb .....	511
2. Home-Office .....	514
III. Informationspflichten und Betroffenenrechte .....	515
IV. Datenschutzerklärung für Mitarbeiter .....	515

## **17. Kapitel** **Werbemaßnahmen und Datenschutz**

*Ursula Illibauer*

I. „Offline“-Werbung .....	518
II. „Online-Werbung“ .....	519
A. Social Media .....	521
B. Telefonwerbung .....	523
C. Elektronische Nachrichten .....	525
1. Einwilligung .....	526
2. Direktwerbung .....	527
3. Ausnahme .....	528
4. Jedenfalls unzulässig .....	530
5. Strafdrohung .....	531
6. Informationspflichten nach dem MedienG und nach dem UWG .....	532
7. Informationspflichten nach dem E-Commerce-Gesetz .....	533
8. Informationspflichten nach Art 13 und 14 DSGVO .....	534
D. Cookies und Behavioral Advertising .....	535
1. ePrivacy-Richtlinie oder DSGVO? .....	537
2. Richtlinien .....	537
3. Umsetzung in das TKG .....	541
4. Logfiles .....	544
5. Location Based Services (Standortdaten) .....	545
III. Einsatz von Auftragsverarbeitern .....	547
IV. Bewerbung fremder Kunden mittels Adressverlagen und Direktmarketingunternehmen .....	547
A. Begriff Adressverlag und Direktmarketingunternehmen .....	548
B. Tätigkeit von Adressverlagen und Direktmarketingunternehmen .....	548
1. Datenermittlung .....	548
2. Datenverwendung .....	549
3. Informationspflicht .....	552
4. Auskunftspflicht und Löschungspflichten, Robinson-Liste .....	552
5. Codes of Conduct .....	553
V. Freiheit der Meinungsäußerung und Informationsfreiheit .....	555

**18. Kapitel  
Forschung**

*Michael Löffler*

I. Sonderstellung von Archiv-, Forschungs- oder statistischen Zwecken .....	559
A. Archivzwecke .....	559
B. Forschungszwecke .....	559
C. Statistische Zwecke .....	560
D. Sonderregelungen der DSGVO .....	560
E. Vorschriften für besondere Verarbeitungssituationen .....	561
1. Öffnungsklauseln für weitere Sonderregelungen .....	562
II. Österreichische Sonderregelungen im DSG .....	562
A. Zulässigkeit von Archiv-, Forschungs- oder statistischen Zwecken .....	563
1. Anonyme Verarbeitungsergebnisse .....	563
a) Verarbeitung öffentlich zugänglicher Daten .....	564
b) Bereits zulässigerweise ermittelte Daten .....	564
c) Pseudonyme Daten ohne rechtliche Möglichkeit zur Identitätsbestimmung .....	565
2. Personenbezogene Verarbeitungsergebnisse/andere Datenquellen .....	565
a) Besondere gesetzliche Vorschriften .....	565
b) Einwilligung betroffener Personen .....	565
c) Genehmigung der DSB .....	566
3. Verpflichtung zur Pseudonymisierung/Anonymisierung .....	569
4. Besondere Kategorien personenbezogener Daten/ strafrechtlich relevante Daten .....	569
5. Einhaltung allgemeiner Bestimmungen der DSGVO .....	569
III. Forschungsorganisationsgesetz .....	570
A. Verhältnis zwischen FOG, DSG und DSGVO .....	570
B. Zulässige Verarbeitungen nach dem FOG .....	571
1. Allgemeine Regelung .....	571
2. „Broad consent“ .....	572
3. Regelungen für spezifische Themen .....	572
C. Grundlegende Datenschutzbestimmungen des FOG .....	573
1. Möglichkeiten des FOG .....	573
IV. Ausnahmen von Datenschutz-Folgenabschätzungen .....	574
A. Ausnahmen der DSFA-AV .....	574
B. Ausnahmen des FOG .....	574
V. Benachrichtigung oder Befragung Betroffener .....	574
VI. Strafbestimmungen .....	576
VII. Checkliste Archiv-, Forschungs- oder statistische Zwecke .....	576

**19. Kapitel  
Rechtsschutz und Sanktionen**

*Thomas Schweiger*

I. Befugnisse der Datenschutzbehörde .....	579
A. Untersuchungsbefugnisse .....	579

B. Abhilfebefugnisse .....	580
1. Warnungen/Verwarnungen/Ermahnungen .....	580
2. Beseitigung von festgestellten Verstößen .....	581
C. Genehmigungs- und Beratungsbefugnisse .....	583
II. Beschwerde an die Datenschutzbehörde .....	583
A. Allgemeines .....	583
B. Voraussetzungen .....	584
C. Beschwerde wegen Verletzung der Geheimhaltungspflicht wegen Verstoß gegen die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art 5 DSGVO oder die Rechtmäßigkeit der Verarbeitung gemäß Art 6 bzw 9 DSGVO .....	587
D. Beschwerde wegen Verletzung der Informationspflicht .....	587
E. Beschwerde wegen Verletzung von Betroffenenrechten .....	588
III. Strafen .....	588
A. Strafen nach dem StGB .....	588
B. Strafen nach DSG .....	589
1. Verwaltungsstrafbestimmung (§ 62 DSG) .....	589
2. Gerichtliche Strafbestimmung (§ 63 DSG) .....	590
C. Strafen nach DSGVO .....	591
1. Allgemeines .....	591
2. Strafraumen 2 % bzw bis EUR 10 Mio .....	591
3. Strafraumen 4 % bzw bis EUR 20 Mio .....	592
D. Strafzumessungsgründe .....	592
E. Verwaltungsstrafverfahren bei der DSB .....	597
F. Verfahrenskosten .....	599
G. Wer erhält die Strafe? .....	599
IV. Das Rechtsmittelverfahren nach Entscheidungen der Datenschutzbehörde .....	601
A. Das Rechtsmittelverfahren vor dem Bundesverwaltungsgericht .....	601
B. Beschwerdegegenstand und die Zuständigkeit .....	602
C. Beschwerdelegitimation .....	602
D. Das Verfahren vor dem Bundesverwaltungsgericht .....	602
E. Das Verfahren für Bescheidbeschwerden .....	603
F. Das Verfahren bei Verletzung der Unterrichtungspflicht gem Art 78 Abs 2 bzw Untätigkeit der Datenschutzbehörde .....	604
G. Das Verfahren bei Verletzung der Entscheidungspflicht durch die Datenschutzbehörde .....	605
V. Anrufung der Zivilgerichte durch Betroffene .....	606
A. Parallele Zuständigkeit .....	606
VI. Schadenersatz nach DSG und DSGVO .....	607
A. Allgemeines zum Schadenersatz .....	607
B. Recht auf Wahrung der Privatsphäre nach § 1328 ABGB .....	612
VII. Sonstige Risiken .....	613
A. Klage wegen unlauterem Wettbewerb .....	613
B. Negative Publicity .....	614



**20. Kapitel**  
**Das Datenschutz-Projekt**

*Hans-Jürgen Pollirer*

I. Einleitung .....	617
II. Checkliste zur Umsetzung der DSGVO .....	619
III. Die Projektschritte im Detail .....	620
A. Phase 1: Projektvorbereitung (Plan) .....	620
1. Management Awareness bilden .....	620
2. Projektteam zusammenstellen .....	621
3. Projektauftrag für das Umsetzungsprojekt einholen .....	622
4. Definition der Zielsetzung .....	622
5. Benötigte Ressourcen und Budget bereitstellen .....	622
6. Auswahl von Projektmanagement-Tools und Datenschutz-Software .....	623
7. Prüfung, ob ein Datenschutzbeauftragter bestellt werden muss .....	625
B. Phase 2: Umsetzung (Do) .....	625
1. Erstellung einer unternehmensweiten Datenschutzpolitik .....	625
2. Umsetzung des Datenschutzprogramms .....	626
3. Bestandsaufnahme bestehender Datenschutzstrukturen .....	626
4. Aufnahme der Verarbeitungstätigkeiten .....	626
5. Erstellung der Verzeichnisse .....	627
6. Prüfung auf Einhaltung der Datenschutzgrundsätze und der Rechtmäßigkeit der Verarbeitung .....	628
7. Überprüfung bestehender bzw Einholung neuer Einwilligungserklärungen .....	628
8. Überarbeitung bzw Erstellung von Betriebsvereinbarungen .....	629
9. Durchführung von Datenschutz-Folgenabschätzungen .....	630
10. Erstellung eines Löschkonzepts .....	632
11. Einrichten von Prozessen und Erstellen von Richtlinien für die Einhaltung der Betroffenenrechte .....	633
12. Prüfung allfällig vorhandener Entscheidungen im Einzelfall inkl Profiling ....	634
13. Durchführung von Risikoanalysen .....	635
14. Umsetzung von Datensicherheitsmaßnahmen (TOM) .....	636
15. Prüfung und Adaptierung bzw Neuabschluss von Auftragsverarbeiter-Verträgen .....	636
16. Prüfung der Einhaltung von Data Protection by Design und Data Protection by Default .....	637
17. Einführung eines Data-Breach-Prozesses .....	638
18. Verpflichtung der Mitarbeiter auf das Datengeheimnis .....	638
19. Prüfung auf Einhaltung der Bestimmungen bei Übermittlung personenbezogener Daten in Drittländer .....	638
20. Ausarbeitung einer Stellenbeschreibung für die Rolle des DSBA .....	639
21. Prüfung, ob die Bestellung eines Vertreters in der EU notwendig ist .....	639
22. Schulung der Mitarbeiter .....	639
C. Phase 3: Überwachung (Check) .....	640
1. Durchführung von Audits .....	640
D. Phase 4: Laufende Verbesserung (Act) .....	641

IV. Praxistipps .....	642
A. Fehleinschätzung des Risikos .....	642
1. Einer reicht für massive Probleme .....	642
2. Sie sind Ziel-1-Gebiet für Cyber-Erpresser! .....	643
B. Projektstart, Projektmanagement .....	643
1. Datenschutzbeauftragter bestellt – und fertig? .....	643
2. Der Datenschutzbeauftragte ist nicht der Datenschutzkoordinator! .....	644
3. Sie schaffen als Datenschutzkoordinator nicht alles alleine! .....	644
4. Ein Datenschutzprojekt muss gemanagt werden. ....	645
5. Die DSGVO ist keine Eintagsfliege .....	645
C. Mitarbeiter als bestimmender Faktor in der Datenschutz-Compliance .....	646
1. Datenschutzrecht braucht motivierte Mitarbeiter am richtigen Platz .....	646
2. Brain-Drain der Mitarbeiter verhindern .....	646
3. Mitarbeiter brauchen Führung .....	646
D. Schulen, Fortbilden, Prüfen .....	647
1. Mitarbeiter in Fachabteilungen benötigen Fortbildung .....	647
2. Mitarbeiter „an der Front“ benötigen Schulungen .....	647
3. Datenschutz-Mitarbeiter und Datenschutzbeauftragte benötigen ein zertifiziertes hohes Ausbildungsniveau .....	648
4. Datenschutz-Mitarbeiter und Datenschutzbeauftragte benötigen Fortbildung und Vernetzung .....	648
5. Data Breaches: Fast zu 100% „menschliches Versagen“ .....	649
E. Datenschutz im Unternehmen institutionalisieren .....	650
1. Arbeitskreis Datenschutz einrichten .....	650
2. Jour-Fixe-Calls durchführen .....	650
3. Datenschutzorganisation im Konzern aufbauen .....	650
4. Betriebsrat rechtzeitig einbinden .....	651
5. Trockenübungen machen .....	651
F. Externe Unterstützung .....	652
1. Externe Anbieter mit Expertise aussuchen .....	652
2. Ein Audit bringt Risiken ans Licht .....	652
3. „Aus den Augen, aus dem Sinn“ bei Auftragsverarbeitern ist sehr gefährlich .....	652
4. Unterstützung durch Datenschutz-Software: Schöne Optik alleine reicht nicht .....	652
G. Neue Datenanwendungen prüfen .....	653
1. Die Hausaufgaben machen .....	653
2. Prüfprozess implementieren .....	654
3. Was man nicht versteht, sollte einen vorsichtig machen .....	654
4. Nicht mit Kanonen auf Spatzen schießen .....	655
 Anhang .....	 657
 Stichwortverzeichnis .....	 673