

---

# Inhaltsverzeichnis

Vorwort .....	V
Abkürzungsverzeichnis .....	XV
Autorenverzeichnis .....	XVII

## Verfahren & Behörden

1. GDPR-Watchdogs: Die Arbeit der Österreichischen Datenschutzbehörde sowie des Europäischen Datenschutzausschusses innerhalb des neuen datenschutzrechtlichen Rahmenwerks ( <i>Christina Maria Schwaiger</i> ) .....	3
1.1. Die Österreichische Datenschutzbehörde .....	5
1.1.1. Europäische Vorgaben zur Aufsichtsbehörde .....	5
1.1.2. Vorbereitungsarbeiten der Österreichischen Datenschutzbehörde .....	18
1.1.3. Erste Erfahrungswerte der Datenschutzbehörde seit 25. 5. 2018 .....	19
1.2. Der Europäische Datenschutzausschuss .....	23
1.2.1. Rückblick Artikel-29-Datenschutzgruppe .....	23
1.2.2. EDSA – Einrichtung und Unabhängigkeit .....	25
1.2.3. Die Geschäftsordnung des Ausschusses .....	26
1.2.4. „Memorandum of Understanding“ .....	26
1.2.5. Vorsitz .....	27
1.2.6. Das Sekretariat des EDSA .....	28
1.2.7. Die Expertenuntergruppen des Europäischen Datenschutzausschusses .....	30
1.2.8. „Track Record“ – wesentliche Arbeiten des EDSA seit 25. 5. 2018 .....	35
1.2.9. Erste Erfahrungen des EDSA seit 25. 5. 2018 .....	41

## Datenschutzbeauftragter

2. Die strategische Positionierung des Datenschutzbeauftragten im Verein ( <i>Renate Grabinger</i> ) .....	47
2.1. Allgemeines zum Datenschutzbeauftragten .....	49
2.1.1. Einleitung .....	49
2.1.2. Der Datenschutzbeauftragte als Teilbereich der Datenschutz-Compliance .....	49
2.1.3. Pflicht zur Benennung eines Datenschutzbeauftragten .....	50
2.1.4. Benennung eines gemeinsamen Datenschutzbeauftragten .....	54
2.2. Strategische Überlegungen zur Benennung eines Datenschutzbeauftragten .....	57
2.2.1. Innerbetriebliche Notwendigkeit versus gesetzliche Verpflichtung .....	57
2.2.2. Strategische Überlegungen am Beispiel des Vereins .....	58
2.3. Anforderungen an den Datenschutzbeauftragten .....	61
2.3.1. Qualifikation .....	61
2.3.2. Verantwortung .....	64
2.3.3. Weisungsfreiheit und Unabhängigkeit .....	66
2.3.4. Interessenkonflikte .....	67
2.3.5. Ressourcenausstattung .....	69

2.4.	Strategische Überlegungen im Hinblick auf die Anforderungen an den Datenschutzbeauftragten .....	73
2.4.1.	Positionierung des Datenschutzbeauftragten in der Organisation .....	73
2.4.2.	Einbindung des Datenschutzbeauftragten in die Organisation .....	74
2.4.3.	Arbeitsweise und Ressourcen des Datenschutzbeauftragten .....	76
2.4.4.	Wegbegleiter des Datenschutzbeauftragten in der Organisationsstruktur .....	79
2.4.5.	Mögliche Zusammenarbeit und Schnittstellen/Rollen in der Organisation .....	80
2.5.	Checkliste für die Prüfung der Notwendigkeit sowie die Benennung eines Datenschutzbeauftragten .....	84
3.	<b>Datenschutz-Management und Datenschutzprozesse unter Berücksichtigung eines Konzerngefüges</b> ( <i>Hannelore Schmidt</i> ) .....	87
3.1.	Datenschutz-Managementsystem .....	88
3.1.1.	Datenschutzrechtliche Regelungen zum DSMS .....	89
3.1.2.	Aufbau eines DSMS .....	92
3.1.3.	Inhalt eines DSMS .....	94
3.2.	Datenschutzorganisation und Datenschutzprozesse unter Berücksichtigung konzernrelevanter Anforderungen .....	123
3.2.1.	Die Unternehmensgruppe – Konzern .....	123
3.2.2.	Personelle Datenschutzorganisation .....	124
3.2.3.	Bestellung eines (Konzern-)Datenschutzbeauftragten und seine Aufgaben .....	124
3.2.4.	Verantwortlicher für den Datenschutz im Unternehmen – Datenschutzbüro .....	126
3.2.5.	Datenschutzkoordinatoren und Datenschutzvertreter .....	126
3.2.6.	Datenschutzprozesse unter Berücksichtigung eines Konzerngefüges .....	127
<b>IT &amp; Blockchain</b>		
4.	<b>Datenschutz und Blockchain: Rechtliche Herausforderungen im Zeitalter exponentieller Technologien</b> ( <i>Guenther Dobrauz-Saldapenna/Philipp Rosenauer</i> ) .....	133
4.1.	Einleitung .....	134
4.2.	Entstehungsgeschichte der Blockchain .....	135
4.2.1.	Funktionsweise der Blockchain .....	135
4.2.2.	Zentrale Wesensmerkmale .....	136
4.3.	Problemstellung .....	137
4.3.1.	Verantwortlicher und Auftragsverarbeiter .....	139
4.3.2.	Transparenz und Zweckbindung .....	142
4.3.3.	Datenminimierung .....	142
4.3.4.	Recht auf Berichtigung .....	143
4.3.5.	Recht auf Vergessenwerden/Recht auf Löschung .....	143
4.3.6.	Auskunftsrecht .....	144
4.3.7.	Automatisierte Entscheidung im Einzelfall .....	145

4.4.	Datenschutzrechtliche Lösungsansätze der Blockchain-Technologie .....	146
4.4.1.	Chamäleon-Hashfunktion .....	147
4.4.2.	„Off-chain“-Datenspeicherung .....	147
4.4.3.	Datenschutz-Overlays .....	147
4.5.	Fazit .....	148

## Datenschutzverträge

5.	Datenschutzverträge ( <i>Michael M. Pachinger</i> ) .....	153
5.1.	Verantwortlichkeit .....	156
5.1.1.	Entscheidung über Zweck und Mittel .....	156
5.1.2.	Art, Umfang, Umstände, Zwecke .....	157
5.1.3.	Nachweis und Vertragsrecht .....	159
5.1.4.	Haftung und Schadenersatz .....	161
5.2.	Gemeinsame Verantwortung – „Joint Controllership“ .....	164
5.2.1.	Allgemein .....	164
5.2.2.	Stellungnahme WP 169 .....	165
5.2.3.	Abgrenzung und Beispiele .....	166
5.2.4.	Aktuelle Judikatur .....	169
5.2.5.	Vertrag zwischen gemeinsam Verantwortlichen (VGV) – wichtige Vertragsklauseln .....	172
5.2.6.	Zurverfügungstellung .....	179
5.2.7.	Gemeinsame Verantwortung und DSFA .....	179
5.2.8.	Sanktionen .....	180
5.3.	Auftragsverarbeitung .....	181
5.3.1.	Allgemeines .....	181
5.3.2.	Stellungnahme WP 169 .....	182
5.3.3.	Abgrenzung und Beispiele .....	184
5.3.4.	Sonderfall Wartungsverträge .....	189
5.3.5.	Eigene datenschutzrechtliche Pflichten .....	193
5.3.6.	Auftragsverarbeitervertrag (AVV) – wichtige Vertragsklauseln .....	194
5.3.7.	Vertrag und elektronisches Format .....	207
5.3.8.	Vertrag oder anderes Rechtsinstrument .....	207
5.3.9.	Vertrag und AGB .....	208
5.3.10.	Sanktionen .....	209
5.4.	Mehrere Verantwortliche – selbstständige Verantwortlichkeit .....	209

## Straf- und Arbeitsrecht

6.	Datenschutzstrafrecht ( <i>Clemens Thiele</i> ) .....	213
6.1.	Strafbare Datenschutzverletzungen .....	216
6.1.1.	Rechtsquellen und Gesetzssystematik .....	217
6.1.2.	Anwendungsvoraussetzungen .....	221
6.1.3.	Besonderheiten .....	242
6.2.	Verwaltungsstrafen nach DSGVO .....	251
6.2.1.	Widerrechtlicher Zugang zur Datenverarbeitung .....	252
6.2.2.	Verletzung des Datengeheimnisses .....	257

6.2.3.	Datenverschaffung unter Vortäuschung falscher Tatsachen im Katastrophenfall .....	261
6.2.4.	Datenschutzwidrige Bildverarbeitung .....	264
6.2.5.	Verweigerung der behördlichen Einschau .....	271
6.3.	Verfahrensrecht .....	275
6.3.1.	Abgrenzung zwischen gerichtlicher und verwaltungsbehördlicher Zuständigkeit .....	275
6.3.2.	Verwaltungsbehördliches Datenschutzstrafverfahren .....	277
6.3.3.	Gerichtliches Datenschutzstrafverfahren .....	284
6.4.	Doppelverfolgungsverbot .....	288
6.4.1.	Strafcharakter der Sanktion .....	288
6.4.2.	Identität .....	290
6.4.3.	Keine Sperrwirkung .....	290
6.5.	Checkliste .....	291
<b>7.</b>	<b>Datenschutz im Beschäftigungskontext (Roland Heinrich) .....</b>	<b>293</b>
7.1.	Personalverwaltung .....	295
7.1.1.	Informationspflichten .....	295
7.1.2.	Rechtsgrundlagen und Einwilligung .....	296
7.1.3.	Datengeheimnis .....	300
7.1.4.	Personalakt .....	301
7.1.5.	Bewerberdaten .....	309
7.2.	Arbeitskräfteüberlassung .....	312
7.2.1.	Allgemeine Einordnung .....	312
7.2.2.	Gemeinsame Verantwortung .....	312
7.3.	Der Datenschutzbeauftragte aus arbeits- und datenschutzrechtlicher Sicht .....	314
7.3.1.	Einordnung des Datenschutzbeauftragten .....	314
7.3.2.	Zuständigkeitsbereich des Datenschutzbeauftragten .....	316
7.3.3.	Verpflichtungen des Datenschutzbeauftragten gegenüber Dritten .....	317
7.3.4.	Gemeinsamer Datenschutzbeauftragter .....	318
7.3.5.	Leitende Stellung des Datenschutzbeauftragten .....	318
7.4.	Datenschutz zwischen Dienstgeber und Betriebsrat .....	319
7.4.1.	Stellung des Betriebsrates .....	319
7.4.2.	Der Betriebsrat als Verantwortlicher .....	320
7.4.3.	Datenweitergabe an Betriebsrat .....	323
7.4.4.	Betriebsrat und gemeinsame Verantwortung iSd Art 26 DSGVO .....	324
7.5.	Betriebsvereinbarungen .....	325
7.5.1.	Betriebsvereinbarungen und DSGVO .....	325
7.5.2.	Betriebsvereinbarung als Einwilligung? .....	326
7.5.3.	Gestaltung von Betriebsvereinbarungen .....	328
7.6.	Anlagen .....	328

## International

<b>8. Rechtliche Absicherung des Datentransfers – insbesondere internationaler Datenübermittlung (Sebastian Meyer/Laura Schulte)</b> .....	<b>335</b>
8.1. Einführung .....	336
8.2. Anwendungsbereich .....	338
8.2.1. Ausgangsfall .....	338
8.2.2. Auftragsverarbeitung und Unterauftragsvergabe .....	339
8.2.3. Konzerninterne grenzüberschreitende Datenverarbeitung .....	340
8.2.4. Internationale Datentransfers und räumlicher Anwendungsbereich .....	341
8.3. Rechtmäßigkeitsanforderungen .....	342
8.3.1. Datenübermittlung auf Basis eines Angemessenheitsbeschlusses .....	342
8.3.2. Geeignete Garantien iSv Art 46 .....	346
8.3.3. Ausnahmetatbestände .....	354
8.4. Datenübermittlung auf der Grundlage drittstaatlicher Anordnungen oder Urteile .....	359
8.4.1. Reichweite und Hintergrund von Art 48 .....	359
8.4.2. Verhältnis von Art 48 zum amerikanischen Cloud-Act .....	360
8.4.3. Absicherung gegen Zugriffe durch Treuhänder-Modelle .....	361

## Strategie & Organisation

<b>9. Datenschutz und Organisation – Praxistipps zu Grundlagen, Organisation und Umsetzung (Johannes Warter)</b> .....	<b>365</b>
9.1. Einleitung .....	367
9.2. Teil 1: Umsetzungsprojekt – vom Ist- zum Sollzustand .....	368
9.2.1. Schwierigkeiten der Materie – notwendiges Wissen .....	369
9.2.2. Implementierungsprojekt – warum Projekt? .....	370
9.2.3. Auswahl der Mitarbeiter .....	370
9.2.4. Projektstart .....	371
9.2.5. Rückendeckung des Managements – „Tone from the Top“ .....	376
9.2.6. Arbeitspakete .....	377
9.2.7. Priorisiertes Vorgehen – risikobasierter Ansatz .....	378
9.2.8. Projektsteuerung .....	379
9.2.9. Mitarbeiterperformance – vier „Trauerphasen“ des Datenschutzes .....	380
9.2.10. Projektmarketing .....	382
9.2.11. Abschlussbericht und Abschlussgespräch – (Übergabe an eine) Regelorganisation .....	383
9.2.12. 13 Tipps zum ausgereiften Projektmanagement nach <i>Kerzner</i> .....	385
9.3. Teil 2: Inhaltliche Anforderungen der DSGVO/des DSG und deren organisatorische Umsetzung .....	385
9.3.1. Rollen und Verantwortlichkeiten .....	386
9.3.2. Einhaltung der Datenschutzgrundsätze .....	390
9.3.3. Exkurs: Grundsatz der Speicherbegrenzung .....	390
9.3.4. Verarbeitungsverzeichnis .....	391
9.3.5. Wahrung der Rechte Betroffener .....	395
9.3.6. Einwilligung .....	398
9.3.7. Einführung von Informationspflichten .....	401

9.3.8. Auftragsverarbeitungsverträge/Verträge gemeinsamer Verantwortlicher .....	403
9.3.9. Einführung des Data-Breach-Prozesses .....	404
9.3.10. Sicherstellung von Datensicherheitsmaßnahmen .....	407
9.3.11. Privacy by Design/Privacy by Default .....	409
9.3.12. Datenschutz-Folgenabschätzung .....	410
9.3.13. Datentransfer in Drittstaaten .....	411
9.3.14. Schulungskonzept .....	411
9.3.15. Datenschutz-Policy – interne Richtlinien .....	412
9.3.16. Internes Kontrollsystem und Audits .....	413
9.4. Teil 3: Wichtige Prinzipien und „Lessons Learned“ .....	414
9.4.1. Datenschutz als „Enabler“ .....	414
9.4.2. KISS-Prinzip .....	415
9.4.3. Einfach starten! .....	415
9.4.4. Plan – Do – Check – Act .....	416
9.4.5. Nicht vor den Karren spannen lassen! .....	416
9.4.6. „Ein System löst keine Probleme“ .....	417
9.4.7. Bauchladen-Prinzip .....	417
9.4.8. Unterstützungsmaßnahmen und Standardisierungen .....	418
9.5. Zusammenfassung und Conclusio .....	419

## Sicherheit

10. Die risikobasierte Umsetzung von Datensicherheitsmaßnahmen in der Praxis von Unternehmen und Behörden ( <i>Thorsten Jost</i> ) .....	423
10.1. Warum die DSGVO aus der Sicht des Angreifers „Sinn macht“ .....	427
10.1.1. „Social Engineering“ als unterschätzte Gefahr für den Schutz von personenbezogenen Daten .....	429
10.1.2. Generelle Sicherheitstipps zur präventiven Abwehr von Angriffen .....	434
10.2. Die Anforderungen der DSGVO an die Datensicherheit .....	435
10.2.1. Technische Sicherheitsmaßnahmen .....	436
10.2.2. Personelle Sicherheitsmaßnahmen .....	436
10.2.3. Organisatorische Sicherheitsmaßnahmen .....	437
10.3. Anwendbare Normen und Best Practices – ein Überblick .....	437
10.3.1. ISO/IEC 27001 .....	438
10.3.2. ISO/IEC 27002 .....	438
10.3.3. ISO/IEC 27018 .....	438
10.3.4. BSI: IT-Grundschutz .....	439
10.3.5. Österreichisches Informationssicherheitshandbuch .....	439
10.3.6. Payment Card Industry Data Security Standard (PCI-DSS) .....	439
10.3.7. Internationale Organisationen für Informationssicherheit .....	440
10.4. Technische und organisatorische Maßnahmen in der Praxis unter Anwendung der ISO 27001 und der Maßnahmenkataloge des BSI-IT-Grundschutzes .....	440
10.4.1. Die vier Schutzziele – Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit .....	441
10.4.2. Sicherheitsmanagement durch ein Informationssicherheits-Managementssystem (ISMS) .....	443

10.4.3. Wesentliche Richtlinien und Möglichkeiten für unternehmens- und behördeninterne Vorgaben zur Datensicherheit .....	445
10.4.4. Pseudonymisierung versus Anonymisierung – Fallstricke in der Praxis .....	448
10.4.5. IT-Notfall- und Krisenmanagement .....	452
10.5. Der risikobasierte Ansatz unter Kombination von Gefährdungs- und Schwachstellenanalyse mit der DSFA .....	468
10.5.1. Was ist ein Risiko aus Datensicherheitssicht? .....	469
10.5.2. Ziele des Sicherheitsrisikomanagements .....	471
10.5.3. Risikomanagement als sich wiederholender Prozess .....	471
10.5.4. Definition des Kontexts für die Risikoidentifikation .....	473
10.5.5. Datensicherheitsrisiken analysieren .....	473
10.5.6. Datensicherheitsrisiken bewerten .....	476
10.5.7. Datensicherheitsrisiken behandeln .....	478
10.5.8. Identifikation von Risiken für Rechte und Freiheiten von Betroffenen unter Anwendung der DSFA .....	479
10.5.9. Die methodische Herangehensweise bei der Bewertung von Risiken für Rechte und Freiheiten von Betroffenen unter Berücksichtigung von Datensicherheitsrisiken .....	480
10.6. Der praxisbezogene Umgang mit Datenpannen .....	483
10.6.1. Was ist eine Datenpanne? .....	483
10.6.2. Vorbereitung, Vorlagen und Prozessgestaltung .....	484
10.6.3. Die Behandlung von Datenpannen im praktischen Prozessablauf .....	489
10.6.4. Resümee .....	492
<b>Stichwortverzeichnis .....</b>	<b>493</b>