

# Inhaltsverzeichnis

Vorwort .....	V
Geleitwort .....	VII
Herausgeberin/Autorinnen und Autoren .....	IX
Abkürzungsverzeichnis .....	XXIII

## **Teil 1: Der Datenschutzbeauftragte in Österreich – Aufgaben und Anforderungen an ein neues Berufsbild**

<b>1. Der Datenschutzbeauftragte gemäß DSGVO/DSG in Österreich (Ségur-Cabanac) .....</b>	<b>1</b>
1.1. Der Datenschutzbeauftragte – in Österreich keine neue Idee, aber nunmehr etabliert .....	1
1.2. Die Bestellung bzw Benennung eines Datenschutzbeauftragten .....	2
1.3. Dauer der Bestellung .....	3
1.4. Wer kann zum Datenschutzbeauftragten bestellt werden? .....	4
1.5. Aufgaben des Datenschutzbeauftragten .....	5
1.6. Die Stellung des Datenschutzbeauftragten .....	7
1.7. Ausreichende Ressourcen für sowie laufende Aus- und Fort- bildung des Datenschutzbeauftragten .....	8
1.8. Kommunikation mit Betroffenen .....	9
1.9. Ansprechperson für die Datenschutzbehörde .....	10
1.10. Resümee .....	10
<b>2. Die Schnittstellenfunktion des Datenschutzbeauftragten zur Behörde: Bisherige Praxiserfahrungen und Anforderungen aus Behördensicht (Schmidl) .....</b>	<b>11</b>
2.1. Vorgaben der DSGVO und des DSG .....	11
2.1.1. Die Aufsichtsbehörde .....	11
2.1.2. Die Aufsichtsbehörde und die Datenschutz- beauftragten .....	12
2.2. Die Zusammenarbeit in der Praxis .....	14
2.2.1. Berät die Datenschutzbehörde auf Anfrage die Datenschutzbeauftragten? .....	14
2.2.2. Muss ein Datenschutzbeauftragter seinen Wohnsitz in Österreich haben? .....	14
2.2.3. Ist der Datenschutzbeauftragte Anlaufstelle für die Datenschutzbehörde in Verfahren? .....	14

2.2.4.	Wer muss einen Datenschutzbeauftragten der Datenschutzbehörde melden? .....	15
2.2.5.	Kann ein Datenschutzbeauftragter als Verant- wortlicher nach § 9 VStG bestellt werden? .....	15
2.2.6.	Die Pflicht zur Zusammenarbeit mit der Behörde ...	16
2.2.7.	Zusammenfassung .....	17
<b>3.</b>	<b>Der Datenschutzbeauftragte im Spannungsfeld zwischen Verant- wortlichen/Auftragsverarbeitern und Betroffenen (Hodžić) .....</b>	<b>17</b>
3.1.	Spannungsfelder .....	18
3.1.1.	Beziehung zum Verantwortlichen bzw Auftrags- verarbeiter .....	18
3.1.2.	Beziehung zum Betroffenen .....	19
3.1.3.	Spannungsfeld Verantwortlicher–Betroffener .....	20
3.1.4.	Spannungsfeld DSBA–Verantwortlicher– Betroffener .....	21
3.2.	Der richtige Umgang .....	22
3.2.1.	Allgemeines .....	22
3.2.2.	Kommunikation mit Betroffenen .....	22
3.2.3.	Kommunikation mit Verantwortlichen/Auftrags- verarbeitern .....	25
3.2.3.1.	Allgemein .....	25
3.2.3.2.	Man kann nicht alles wissen .....	26
3.2.3.3.	Zuverlässigkeit .....	26
3.3.	Fazit .....	27
<b>4.</b>	<b>Mediation in Datenschutzangelegenheiten (Wanderer).....</b>	<b>27</b>
4.1.	Warum ist Mediation für Datenschutzkonflikte geeignet? .....	27
4.1.1.	Datenschutz gilt nicht absolut und berücksichtigt unterschiedliche Interessenlagen .....	27
4.1.2.	Einbeziehung der Interessen des Betroffenen im Bereich des Datenschutzrechts .....	28
4.2.	Allgemeines zur Mediation .....	28
4.3.	Unterschiede zu anderen Verfahren .....	29
4.3.1.	Zivilgericht .....	29
4.3.2.	Datenschutzbehörde .....	29
4.4.	Mögliche Settings .....	29
4.4.1.	(Drohende) schadenersatzrechtliche Klage gegen Unternehmen .....	29
4.4.2.	Betroffener beschwert sich über die Verletzung seiner Rechte .....	31
4.4.3.	Datenschutzmediation in Verhaltensregeln/ Codes of Conduct .....	31

4.5.	Motivationen des Betroffenen .....	31
4.5.1.	Geld als Motivation .....	31
4.5.2.	Betroffener will sich für erlittenes Unrecht revanchieren .....	31
4.5.3.	Betroffener will sich einbringen und ernst genommen werden .....	32
4.6.	Motivation aus Sicht des Unternehmens .....	32
4.7.	Vorteile für die Parteien .....	34
4.7.1.	Kosten .....	34
4.7.2.	Dauer .....	34
4.7.3.	Selbstbestimmtheit .....	34
4.7.4.	Kein Gesichtsverlust/keine negative PR für Unternehmen .....	35
4.8.	Mediation im Alltag des Datenschutzbeauftragten .....	36
4.8.1.	Innerbetriebliche Konfliktfelder .....	36
4.8.2.	Konflikte zwischen dem Unternehmen und Dritten .....	38
4.8.3.	Exkurs: Der Weg zum Mediator – Voraussetzungen für die Ausübung der Mediation als (selbständiger) Mediator .....	39
4.9.	Vom Konfliktgegner zum Kooperationspartner .....	40
<b>5.</b>	<b>Aufgaben und Ausbildungsinhalte eines neuen Berufsbildes</b> <i>(Riedl)</i> .....	40
5.1.	Allgemeines .....	40
5.2.	Berufliche Qualifikation, insbesondere Fachwissen .....	41
5.3.	Grundlagen der Fähigkeit zur Erfüllung der Aufgaben .....	43
5.4.	Aus- und Weiterbildung .....	43
<b>6.</b>	<b>Überwachung der Einhaltung der DSGVO: Durchführung von</b> <b>Datenschutz-Audits durch den Datenschutzbeauftragten</b> <i>(Kastelitz/Gamper)</i> .....	45
6.1.	Einleitung .....	45
6.1.1.	Audits: Ein (kurzer) Überblick .....	46
6.1.2.	Datenschutz-Audit: Was ist das? .....	48
6.1.2.1.	Warum Datenschutz-Audits verpflichtend durchzuführen sind .....	49
6.2.	Die Überwachungsaufgaben des Datenschutzbeauftragten .....	51
6.2.1.	Überwachung der Datenschutz-Compliance durch den Datenschutzbeauftragten .....	52
6.2.2.	Abgrenzung der Datenschutz-Audits zum Internen Kontrollsystem .....	55

6.3.	Datenschutz-Auditierung durch den Datenschutz-beauftragten .....	57
6.3.1.	Das Auditprogramm: Dort anfangen, wo es am nötigsten ist .....	57
6.3.2.	Risikomanagement als Grundlage für das Auditprogramm .....	57
6.3.3.	Nach dem Audit ist vor dem Audit: Datenschutzmanagement als Prozess .....	58
6.4.	Planung eines Datenschutz-Audits aus Sicht des Datenschutzbeauftragten .....	59
6.4.1.	Ablauf eines Audits .....	59
6.4.2.	Audit-Ziele: Nicht alles auf einmal wollen .....	60
6.4.2.1.	Es gibt für alles ein erstes Mal .....	61
6.4.3.	Audit-Kriterium (Vorbereitung) .....	61
6.4.3.1.	Akzeptanz schaffen statt Widerstände überwinden ...	62
6.4.4.	Audit-Nachweis (Durchführung) .....	62
6.4.5.	Audit-Feststellung (Durchführung und Nachbereitung) .....	63
6.4.6.	Audit-Schlussfolgerungen (Nachbereitung, Berichtslegung) .....	63
6.4.7.	Abschluss: Ergebnisse und Präsentation .....	63
6.5.	Grundmuster eines Datenschutz-Audit-Prüfkatalogs (Audit-Checkliste) .....	64
<b>7.</b>	<b>Haftung des Datenschutzbeauftragten (Riedl) .....</b>	<b>67</b>
7.1.	Allgemeines .....	67
7.2.	Interner DSBA .....	69
7.3.	Externer DSBA .....	70
7.4.	DSBA als verantwortlicher Beauftragter? .....	70
<b>8.</b>	<b>Datenschutzbeauftragter und Interessenkonflikte (Riedl) .....</b>	<b>71</b>
8.1.	Allgemeines .....	71
8.2.	Positionen mit Interessenkonflikt .....	72
8.3.	Sonstige mögliche Interessenkonflikte .....	73
8.3.1.	Interessenkonflikte aufgrund weiterer Aufgaben ....	73
8.3.2.	Betriebsrat als DSBA .....	74
8.3.3.	Naheverhältnis und Interessenkonflikte .....	75
8.3.4.	Interessenkonflikte bei externen DSBA .....	75
<b>9.</b>	<b>Die arbeitsrechtliche Stellung/Schutz/Kündigungsschutz des DSBA (Riedl) .....</b>	<b>76</b>
9.1.	Allgemeines .....	76
9.2.	Weisungsfreiheit .....	78
9.3.	Benachteiligungsverbot und Abberufungsschutz .....	79
9.4.	Bericht an höchste Managementebene .....	81

<b>10. Der externe Datenschutzbeauftragte (Mangelberger)</b> .....	82
10.1. Ausgangslage .....	82
10.1.1. Hintergrund .....	82
10.2. Exkurs: Der externe DSBA im öffentlichen Bereich .....	85
10.3. (Berufsrechtliche) Voraussetzungen: Wer kann (externer) Datenschutzbeauftragter werden? .....	87
10.3.1. Anforderungen nach der DSGVO .....	87
10.3.2. Berufsrechtliche Anforderungen nach österreichischem Recht .....	89
10.4. Die juristische Person als externer DSBA .....	92
10.5. Vor- und Nachteile der Bestellung eines externen DSBA .....	93
10.5.1. Ressourceneinsatz .....	93
10.5.2. Vermeidung von Interessenkonflikten .....	93
10.5.3. Blick von außen .....	94
10.5.4. Haftung des externen DSBA .....	95
10.5.5. Schulung und Sensibilisierung .....	96
10.6. Fazit .....	97
<b>Teil 2: Der DSBA im Konzern/in der Unternehmensgruppe/ im Großunternehmen</b>	
<b>1. Der Datenschutzbeauftragte im internationalen Konzern/ in der Unternehmensgruppe (Riedl)</b> .....	99
1.1. Allgemeines .....	99
1.2. Gemeinsamer Datenschutzbeauftragter .....	99
1.2.1. Unternehmensgruppe .....	99
1.2.2. Niederlassung .....	100
1.2.3. Leichte Erreichbarkeit .....	101
<b>2. Fragen der Governance: Konzerndatenschutzbeauftragter und die Zusammenarbeit/Abgrenzung der Arbeit zu Datenschutz- koordinatoren (oder jede andere Bezeichnung) und der operativen Arbeit (Riedl)</b> .....	102
<b>3. Zusammenarbeit mit Compliance/Risk Management/IT/ anderen Abteilungen im Unternehmen (Riedl)</b> .....	105
<b>Teil 3: Der DSB in KMU und kleinen Vereinen (Scheichenbauer/Windholz)</b>	
<b>1. Einleitung</b> .....	107
<b>2. Allgemeines zur Benennungspflicht</b> .....	107
<b>3. Was versteht man unter der Kerntätigkeit?</b> .....	108
3.1. Wann liegt eine umfangreiche Verarbeitung von besonderen Datenkategorien oder strafrechtlich relevanten Daten vor? .....	109

3.2.	Was ist unter regelmäßiger, systematischer und umfangreicher Überwachung zu verstehen? .....	112
<b>4.</b>	<b>Vereine, die möglicherweise eine Bestellpflicht trifft</b> .....	<b>112</b>
4.1.	Fallgruppen: Vereine, die (möglicherweise) eine Bestellpflicht aufgrund umfangreicher Verarbeitung besonderer Datenkategorien/Strafdaten trifft .....	113
4.1.1.	Umfangreiche systematische oder regelmäßige Überwachung durch Vereine? .....	113
4.1.2.	Vorgehensweise bei Prüfung der Bestellpflicht .....	114
4.2.	Gemeinsamer DSBA für mehrere Vereine/Vereinsverbände? ....	120
<b>5.</b>	<b>KMU, die möglicherweise eine Bestellpflicht trifft</b> .....	<b>122</b>
5.1.	Kerntätigkeit und umfangreiche Verarbeitung von sensiblen Daten .....	122
5.2.	Kerntätigkeit und umfangreiche Überwachung .....	123
5.3.	Fallgruppen KMU mit möglicher Bestellpflicht .....	123
<b>6.</b>	<b>Umsetzung im ersten Jahr</b> .....	<b>124</b>
6.1.	Weichenstellung .....	124
6.2.	Evaluierung .....	126
6.3.	Lenkung .....	127
6.3.1.	Exkurs: Technische und organisatorische Maßnahmen .....	128
6.4.	Überprüfung .....	128
6.5.	Ständige Tätigkeiten .....	129
6.6.	Laufender Betrieb .....	129

**Teil 4: Der Datenschutzbeauftragte in ausgewählten Branchen**

<b>1.</b>	<b>Datenschutzbeauftragter in der Bank (Wagner)</b> .....	<b>131</b>
1.1.	Einleitung .....	131
1.2.	Rechtsgrundlagen .....	131
1.2.1.	Rechtliche Verpflichtungen (Art 6 Abs 1 Buchst c DSGVO) .....	131
1.2.1.1.	Finanzmarkt-Geldwäsche-Gesetz (FM-GwG) .....	132
1.2.1.2.	Wertpapieraufsichtsgesetz (WAG) .....	133
1.2.2.	Vertragserfüllung (Art 6 Abs 1 Buchst b DSGVO) ....	133
1.2.3.	Einwilligung (Art 6 Abs 1 Buchst a DSGVO) .....	133
1.2.3.1.	Besondere Kategorien von personenbezogenen Daten .....	134
1.2.4.	Einwilligung für Marketingzwecke .....	134
1.2.4.1.	Bonitätsprüfung im Onlineprozess .....	135
1.2.4.2.	Berechtigtes Interesse (Art 6 Abs 1 Buchst f DSGVO) .....	136

1.2.4.3.	Warnliste und Klein-Kreditevidenz .....	136
1.2.4.4.	Betrugsprävention und -bekämpfung .....	137
1.2.4.5.	Videoüberwachung .....	137
1.2.4.6.	Marketing .....	138
1.2.5.	Sonderfall Telefonaufzeichnung .....	138
1.3.	Informationspflicht gemäß Art 13 f DSGVO .....	138
1.4.	Datenauskunft und Datenübertragbarkeit .....	139
1.4.1.	Datenauskunft .....	139
1.4.2.	Datenübertragbarkeit .....	140
1.5.	Löschung und Anonymisierung von Daten .....	140
1.5.1.	Automatische Löschung und Anonymisierung .....	140
1.5.2.	Ausnahmen von der automatischen Löschung und Anonymisierung .....	141
1.5.2.1.	Verlorene Sparbücher .....	141
1.5.2.2.	Gekündigte Konten .....	141
1.5.2.3.	Verjährte Forderungen .....	141
1.5.2.4.	Steuerprüfung .....	141
1.5.2.5.	Forderungseinlösung .....	142
1.5.2.6.	Betrugsfälle .....	142
1.5.3.	Löschung und Anonymisierung auf Kundenantrag ...	142
1.5.3.1.	Vertrag kommt nicht zustande, Antrag wird zurückgezogen .....	142
1.5.3.2.	Rechtsfallkunden .....	142
1.5.3.3.	Löschung von Bewerberdaten .....	142
1.5.3.4.	Löschung von Telefonaufzeichnungen .....	142
1.5.3.5.	Löschauftrag direkt nach Kontoschließung .....	143
1.5.3.6.	Sonstiges .....	143
1.6.	Datenschutzbeauftragter .....	143
1.7.	Fragebogen für Projekte und IT-Systeme .....	144
<b>2.</b>	<b>Der Datenschutzbeauftragte im Gesundheitsbereich (<i>Vielhaber</i>).....</b>	<b>146</b>
2.1.	Einleitung .....	146
2.2.	Anwendbarkeit der DSGVO auf Patientendaten in digitaler Form und Papierform .....	146
2.3.	Wichtige Kategorien personenbezogener Daten für den Gesundheitsbereich .....	147
2.4.	Kriterien für die Pflicht zur Bestellung eines Datenschutz- beauftragten im Gesundheitsbereich .....	148
2.4.1.	Kriterien in der DSGVO .....	148
2.4.2.	Kriterien im FOG .....	150
2.5.	Spezielle Aufgaben des Datenschutzbeauftragten im Gesund- heitsbereich .....	150

2.6.	Wichtige Bestimmungen für Datenschutzbeauftragte im Gesundheitsbereich .....	150
2.6.1.	Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten in der DSGVO .....	150
2.6.2.	DSFA-V .....	154
2.6.3.	Netz- und Informationssystemsicherheitsgesetz – NISG .....	154
2.6.4.	Berufsrechte .....	155
2.6.5.	KAKuG .....	156
2.6.6.	Gesundheitstelematikgesetz 2012 – GTelG 2012 .....	156
2.6.7.	Landesgesetze .....	157
2.7.	Zusammenfassung .....	158
<b>3.</b>	<b>Der Datenschutzbeauftragte im Telekom-Bereich – Herausforderung Telekommunikations-/IT-Branche (Leschanz) .....</b>	<b>158</b>
3.1.	Allgemeines .....	158
3.2.	Awareness von Kunden .....	159
3.3.	Hohe Innovationskraft .....	160
3.4.	Data Driven Company .....	160
3.5.	Strengere Regulierung .....	160
3.6.	Hohe Agilität .....	161
3.7.	TKG 2003 und Datenschutz .....	161
3.7.1.	Behördenauskunft .....	162
3.7.2.	Datenweitergabe an Betreiber von Notrufdiensten ....	162
3.7.3.	Eigene Datenkategorien .....	163
3.7.4.	Unerbetene Nachrichten .....	163
3.7.5.	Kommunikationsgeheimnis .....	163
3.7.6.	Data Breach .....	164
3.7.7.	Auskünfte an Behörden .....	164
3.8.	E-Privacy .....	164
3.9.	Data Retention .....	165
3.10.	Code of Conduct .....	165
<b>4.</b>	<b>Der Datenschutzbeauftragte im Medienunternehmen (Rauch) .....</b>	<b>166</b>
4.1.	Abgrenzung Datenschutz gegenüber der Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit .....	166
4.2.	Keine journalistischen Daten .....	169
4.3.	Journalistische Daten .....	169
4.4.	Journalistische Daten ... oder doch nicht? .....	169
4.5.	Chamäleon-Daten .....	172
4.6.	Internetauftritt des Medienunternehmens .....	173
4.6.1.	Berichte/Reportagen .....	174
4.6.2.	Werbung und Sonstiges .....	174



4.6.2.1.	Werbung .....	174
4.6.2.2.	Ausspielung durch den Werbetreibenden selbst .....	175
4.6.2.3.	Ausspielung durch den Werbetreibenden .....	175
4.6.3.	Einbindung von „Social Media“ .....	177
4.7.	Fazit .....	179
<b>5.</b>	<b>Der Datenschutzbeauftragte in Infrastrukturunternehmen am Beispiel eines Flughafens (<i>Ruf</i>) .....</b>	<b>180</b>
5.1.	Allgemeines .....	180
5.2.	Die Rolle des Flughafens im Rahmen der Bodenabfertigung .....	181
5.3.	Check-In .....	182
5.4.	Gepäckabfertigung .....	183
5.5.	Bordkartenkontrolle vor der Sicherheitskontrolle .....	184
5.6.	Bordkartenkontrolle am Gate .....	184
5.7.	Schlussbemerkung .....	184
<b>6.</b>	<b>Der Datenschutzbeauftragte in gemeinnützigen Unternehmen (<i>Gudenus</i>) .....</b>	<b>184</b>
6.1.	Allgemeines .....	184
6.2.	Spezifika der gemeinnützigen Beratungs- und Personalüberlassungsunternehmen .....	185
6.3.	Tipps für die Umsetzungsphase .....	188
6.4.	Schlussbemerkung .....	198
<b>7.</b>	<b>Der Datenschutzbeauftragte im öffentlichen Bereich (<i>Hild</i>) .....</b>	<b>199</b>
7.1.	Länderspezifische Umsetzung und Besonderheiten .....	199
7.2.	Die Bestellung des Datenschutzbeauftragten .....	199
7.2.1.	Die Ernennung .....	200
7.2.1.1.	Eigener Mitarbeiter .....	200
7.2.1.2.	Externer Datenschutzbeauftragter .....	201
7.2.1.3.	Teilzeitbeschäftigte Datenschutzbeauftragte, Daten- schutzbeauftragter als Nebenbeschäftigung .....	202
7.2.2.	Mehrere Datenschutzbeauftragte oder Mitarbeiter eines Datenschutzbeauftragten .....	203
7.2.3.	Veröffentlichung und Übermittlung der Kontaktdaten .....	204
7.2.3.1.	Veröffentlichung .....	204
7.2.3.2.	Übermittlung der Kontaktdaten an die Daten- schutzbehörde .....	205
7.3.	Die Stellung des Datenschutzbeauftragten .....	205
7.3.1.	Unabhängig, weisungsfrei .....	205
7.3.1.1.	Unabhängig = unabsetzbar und unversetzbar? .....	206
7.3.1.2.	Weisungsfrei .....	207
7.3.1.3.	Unvereinbarkeiten .....	207

7.4.	Die Pflichten des Verantwortlichen .....	208
7.4.1.	Organisatorische Eingliederung .....	208
7.4.2.	Ressourcen .....	209
7.4.3.	Einbindung .....	210
7.4.4.	Unterstützung .....	210
7.4.5.	Schulung .....	210
7.4.6.	Sonderfall Nebenbeschäftigung als Datenschutz- beauftragter beim selben Verantwortlichen des öffentlichen Bereichs .....	211
7.5.	Die Pflichten des Datenschutzbeauftragten .....	211
7.5.1.	Beratung des Verantwortlichen .....	211
7.5.1.1.	Beratung de lege lata .....	211
7.5.1.2.	Beratung de lege ferenda .....	212
7.5.1.3.	Verschwiegenheitspflicht .....	212
7.5.2.	Berichtspflicht? Unterrichtsrecht .....	213
7.5.3.	Beratung der Betroffenen/Anrufungsrecht .....	214
7.5.4.	Interessenkonflikte .....	215
7.5.5.	Das Verzeichnis der Datenverarbeitungen .....	215
7.5.6.	Mitwirkung bei einer Datenschutzfolgeabschätzung	216
7.5.7.	Mitwirkung bei einer Konsultation der Daten- schutzbehörde .....	216
7.5.8.	Kontakt/Zusammenarbeit mit der Datenschutz- behörde .....	217
7.5.9.	Austausch zwischen den Datenschutzbeauftragten ....	217
7.5.10.	Kontrolle/Überwachung der Einhaltung der DSGVO .....	218
7.5.11.	Schulung .....	218
7.5.12.	Fortbildung .....	218
Anhang 1	.....	221
Anhang 2	.....	227
Anhang 3	.....	253
Stichwortverzeichnis	.....	257