

# Datenschutz-Audit

Recht–Organisation–Prozess–IT

Der Praxisleitfaden zur  
Datenschutz-Grundverordnung

herausgegeben von  
**Dr. Michael M. Pachinger**  
**Georg Beham, MSc**



# Inhaltsverzeichnis

Vorwort .....	V
Glossar .....	XI
Literaturverzeichnis .....	XIII
Autorenverzeichnis .....	XV
<b>1. Einführung .....</b>	<b>1</b>
1.1 Die Datenschutz-Grundverordnung (DSGVO) .....	3
1.2 Accountability als Grundlage verpflichtender Datenschutz-Audits .....	3
1.3 Das österreichische Datenschutzgesetz (DSG 2000) .....	4
<b>2. Grundlagen eines Audits .....</b>	<b>7</b>
2.1 Einleitung .....	7
2.2 Begriffsdefinition .....	8
2.2.1 Handelnde Parteien eines Audits .....	8
2.2.2 Auditkriterien und -ergebnisse .....	9
2.2.3 Auditvarianten .....	10
2.3 Grundsätze eines Audits .....	11
2.4 Planung eines Audits .....	11
2.4.1 Auditprogramm .....	12
2.4.2 Zeitmanagement beim Audit .....	15
2.5 Auditablauf .....	17
2.5.1 Durchführen des Eröffnungsgespräches .....	17
2.5.2 Durchführen des Audits .....	18
2.5.3 Audittools .....	20
2.5.4 Kommunikation während des Audits .....	22
2.5.5 Abschlussgespräch .....	23
2.6 Auditbericht .....	24
2.7 Nachbearbeitung von Audits .....	25
<b>3. Kontrollbereiche als Basis für das Datenschutz-Audit .....</b>	<b>27</b>
3.1 Gliederung .....	27
3.1.1 Kontrollbereiche .....	27
3.1.2 Verpflichtungen .....	27
3.1.3 Kontrollen .....	27
3.1.4 Kontrollgruppen .....	28
3.1.5 Kontrolluntergruppen .....	28
3.2 Beschreibung der Kontrollgruppen .....	28
3.2.1 Kontrollgruppe: Anwendungsbereich DSGVO .....	28
3.2.2 Kontrollgruppe: Betroffenenrechte .....	29
3.2.3 Kontrollgruppe: Aufbewahrung von Daten .....	29

3.2.4	Kontrollgruppe: Datenschutz-Folgenabschätzung.....	30
3.2.5	Kontrollgruppe: Datenschutzkonzept und -management .....	30
3.2.6	Kontrollgruppe: Datensicherheitsmaßnahmen .....	30
3.2.7	Kontrollgruppe: Datensparsamkeit .....	31
3.2.8	Kontrollgruppe: Datenübermittlung .....	31
3.2.9	Kontrollgruppe: Datenvorfall .....	31
3.2.10	Kontrollgruppe: Informationspflichten .....	31
3.2.11	Kontrollgruppe: Rechtmäßigkeit.....	32
3.2.12	Kontrollgruppe: Verantwortlichkeiten .....	32
<b>4.</b>	<b>Kontrollbereich Recht</b>	
4.1	Kontrollgruppe: Anwendungsbereich DSGVO .....	33
4.1.1	Kontrolluntergruppe: Datenklassifikation.....	34
4.2	Kontrollgruppe: Betroffenenrechte.....	35
4.3	Kontrollgruppe: Aufbewahrung von Daten .....	36
4.4	Kontrollgruppe: Datenschutz-Folgenabschätzung .....	37
4.4.1	Kontrolluntergruppe: Maßnahmen .....	39
4.5	Kontrollgruppe: Datenschutzkonzept und -management .....	43
4.6	Kontrollgruppe: Datenübermittlung .....	44
4.6.1	Genehmigung der Datenübermittlung .....	46
4.6.2	Kontrolluntergruppe: Zulässigkeit.....	48
4.7	Kontrollgruppe: Informationspflichten.....	52
4.7.1	Kontrolluntergruppe: Datenverarbeitung .....	53
4.7.2	Kontrolluntergruppe: Verfahren .....	53
4.8	Kontrollgruppe: Rechtmäßigkeit.....	54
4.8.1	Kontrolluntergruppe: Datenklassifikation.....	60
4.8.2	Kontrolluntergruppe: Einwilligung .....	63
4.8.3	Kontrolluntergruppe: Prüfpflicht .....	66
4.8.4	Kontrolluntergruppe: Zweckbindung .....	68
4.9	Kontrollgruppe: Verantwortlichkeiten .....	69
4.9.1	Kontrolluntergruppe: Gemeinsame Datenverarbeitung .....	69
<b>5.</b>	<b>Kontrollbereich Prozess</b>	
5.1	Kontrollgruppe: Anwendungsbereich DSGVO .....	73
5.1.1	Kontrolluntergruppe: Datenklassifikation.....	74
5.2	Kontrollgruppe: Betroffenenrechte.....	75
5.2.1	Kontrolluntergruppe: Datensparsamkeit.....	79
5.2.2	Kontrolluntergruppe: Informationspflicht .....	80
5.2.3	Kontrolluntergruppe: Löschung .....	86
5.2.4	Kontrolluntergruppe: Richtigstellung.....	90
5.2.5	Kontrolluntergruppe: Widerspruch .....	93
5.3	Kontrollgruppe: Aufbewahrung von Daten .....	93
5.4	Kontrollgruppe: Datenschutzkonzept und -management .....	94

5.4.1	Kontrolluntergruppe: Dokumentation und Nachweise .....	95
5.5	Kontrollgruppe: Datensparsamkeit.....	97
5.6	Kontrollgruppe: Datenübermittlung .....	98
5.7	Kontrollgruppe: Datenvorfall .....	99
5.7.1	Kontrolluntergruppe: Dokumentation.....	102
5.7.2	Kontrolluntergruppe: Mitteilungspflicht.....	103
5.8	Kontrollgruppe: Informationspflichten.....	108
5.8.1	Kontrolluntergruppe: Widerspruchsrecht .....	110
5.8.2	Kontrolluntergruppe: Datenverarbeitung .....	114
5.9	Kontrollgruppe: Rechtmäßigkeit.....	118
5.9.1	Kontrolluntergruppe: Einwilligung .....	118
5.9.2	Kontrolluntergruppe: Prüfpflicht .....	119
5.10	Kontrollgruppe: Verantwortlichkeiten.....	120
5.10.1	Kontrolluntergruppe: Datenverarbeitung .....	120
<b>6. Kontrollbereich Organisation</b>		
6.1	Kontrollgruppe: Datenschutzkonzept und -management .....	123
6.1.1	Kontrolluntergruppe: Datenschutzbeauftragter .....	125
6.1.2	Kontrolluntergruppe: Leitende Organe .....	131
6.1.3	Kontrolluntergruppe: Risikobewertung.....	136
6.1.4	Kontrolluntergruppe: Verschwiegenheit .....	139
6.2	Kontrollgruppe: Verantwortlichkeiten.....	140
6.2.1	Kontrolluntergruppe: Auftragsverarbeitung .....	142
6.2.2	Kontrolluntergruppe: Datenverarbeitung .....	145
<b>7. Kontrollbereich IT</b>		
7.1	Kontrollgruppe: Aufbewahrung von Daten .....	149
7.1.1	Kontrolluntergruppe: Aufbewahrungszeiten.....	151
7.1.2	Kontrolluntergruppe: Sperr- und Löschkonzept.....	152
7.1.3	Kontrolluntergruppe: Protokollierung (Logdaten) .....	154
7.2	Kontrollgruppe: Datenschutzkonzept und -management .....	157
7.2.1	Kontrolluntergruppe: Richtlinien und Nachweise .....	157
7.3	Kontrollgruppe: Datensicherheitsmaßnahmen .....	159
7.3.1	Kontrolluntergruppe: Aufgabenzuordnung und Belehrung.....	160
7.3.2	Kontrolluntergruppe: Risikobewertung.....	161
7.3.3	Kontrolluntergruppe: Datenklassifikation.....	163
7.3.4	Kontrolluntergruppe: Zugriffskonzept.....	164
7.3.5	Kontrolluntergruppe: Netzwerksicherheit.....	171
7.3.6	Kontrolluntergruppe: Zutrittskonzept .....	172
7.3.7	Kontrolluntergruppe: Verfügbarkeit.....	175
7.3.8	Kontrolluntergruppe: Integrität.....	178
7.3.9	Kontrolluntergruppe: Belastbarkeit (Performance).....	179
7.3.10	Kontrolluntergruppe: Kommunikationssicherheit .....	180

7.3.11 Kontrolluntergruppe: Protokollierung (Logging) .....	181
7.4 Kontrollgruppe: Datensparsamkeit.....	183
7.5 Kontrollgruppe: Datenübermittlung .....	185
<b>8. Verhaltensregeln und Zertifizierungen</b>	
8.1 ISAE 3000.....	190
8.2 Das Europäische Datenschutz-Gütesiegel „EuroPriSe“ .....	192
8.3 ISO 27001 mit Schwerpunkt Datenschutz .....	193
<b>Abbildungsverzeichnis</b> .....	195
<b>Stichwortverzeichnis</b> .....	197