

# Datenschutz-Audit

Recht – Organisation – Prozess – IT

## Der Praxisleitfaden zur Datenschutz-Grundverordnung

2., aktualisierte Auflage

HERAUSGEGEBEN VON

Dr. Michael M. Pachinger  
Georg Beham, MSc

DIE AUTOREN

Dr. Michael M. Pachinger  
Georg Beham, MSc  
Thorsten Jost  
Peter Kleebauer, MSc



---

# Inhaltsverzeichnis

Vorwort.....	V
Glossar.....	XI
Literaturverzeichnis.....	XIII
Autorenverzeichnis.....	XV
<b>1. Einführung .....</b>	<b>1</b>
1.1 Die Datenschutz-Grundverordnung (DSGVO).....	2
1.2 Accountability als Grundlage verpflichtender Datenschutz-Audits.....	3
1.3 Das österreichische Datenschutzrecht .....	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.....	22
2.6 Auditbericht .....	23
2.7 Nachbearbeitung von Audits .....	24
<b>3. Kontrollbereiche als Basis für das Datenschutz-Audit .....</b>	<b>25</b>
3.1 Gliederung.....	25
3.1.1 Kontrollbereiche .....	25
3.1.2 Verpflichtungen .....	25
3.1.3 Kontrollen .....	25
3.1.4 Kontrollgruppen.....	26
3.1.5 Kontrolluntergruppen .....	26
3.2 Beschreibung der Kontrollgruppen.....	26
3.2.1 Kontrollgruppe: Anwendungsbereich DSGVO.....	26
3.2.2 Kontrollgruppe: Betroffenenrechte .....	27
3.2.3 Kontrollgruppe: Aufbewahrung von Daten.....	27

3.2.4	Kontrollgruppe: Datenschutz-Folgenabschätzung.....	28
3.2.5	Kontrollgruppe: Datenschutzkonzept und -management .....	28
3.2.6	Kontrollgruppe: Datensicherheitsmaßnahmen.....	28
3.2.7	Kontrollgruppe: Datensparsamkeit .....	28
3.2.8	Kontrollgruppe: Datenübermittlung .....	29
3.2.9	Kontrollgruppe: Datenvorfall .....	29
3.2.10	Kontrollgruppe: Informationspflichten.....	29
3.2.11	Kontrollgruppe: Rechtmäßigkeit.....	29
3.2.12	Kontrollgruppe: Verantwortlichkeiten .....	29
3.2.13	Kontrollgruppe: Nationales Datenschutzrecht.....	30
<b>4.</b>	<b>Kontrollbereich Recht .....</b>	<b>31</b>
4.1	Kontrollgruppe: Anwendungsbereich DSGVO .....	31
4.1.1	Kontrolluntergruppe: Datenklassifikation .....	32
4.2	Kontrollgruppe: Betroffenenrechte .....	33
4.3	Kontrollgruppe: Aufbewahrung von Daten.....	35
4.4	Kontrollgruppe: Datenschutz-Folgenabschätzung.....	36
4.4.1	Kontrolluntergruppe: Maßnahmen.....	39
4.5	Kontrollgruppe: Datenschutzkonzept und -management.....	42
4.6	Kontrollgruppe: Datenübermittlung.....	43
4.6.1	Kontrolluntergruppe: Zulässigkeit .....	44
4.7	Kontrollgruppe: Informationspflichten .....	49
4.7.1	Kontrolluntergruppe: Datenverarbeitung .....	51
4.7.2	Kontrolluntergruppe: Verfahren.....	51
4.8	Kontrollgruppe: Rechtmäßigkeit .....	52
4.8.1	Kontrolluntergruppe: Datenklassifikation .....	56
4.8.2	Kontrolluntergruppe: Einwilligung und weitere Rechtsgrundlagen .....	59
4.8.3	Kontrolluntergruppe: Prüfpflicht .....	63
4.8.4	Kontrolluntergruppe: Zweckbindung .....	65
4.9	Kontrollgruppe: Verantwortlichkeiten.....	65
4.9.1	Kontrolluntergruppe: Gemeinsame Datenverarbeitung .....	66
4.10	Kontrollgruppe: Nationales Datenschutzrecht .....	67
<b>5.</b>	<b>Kontrollbereich Prozess .....</b>	<b>79</b>
5.1	Kontrollgruppe: Anwendungsbereich DSGVO .....	79
5.1.1	Kontrolluntergruppe: Datenklassifikation .....	80
5.2	Kontrollgruppe: Betroffenenrechte .....	81
5.2.1	Kontrolluntergruppe: Datensparsamkeit .....	84
5.2.2	Kontrolluntergruppe: Informationspflicht .....	85
5.2.3	Kontrolluntergruppe: Löschung.....	90
5.2.4	Kontrolluntergruppe: Richtigstellung.....	94
5.2.5	Kontrolluntergruppe: Widerspruch.....	97

5.3	Kontrollgruppe: Aufbewahrung von Daten .....	98
5.4	Kontrollgruppe: Datenschutzkonzept und -management.....	98
5.4.1	Kontrolluntergruppe: Dokumentation und Nachweise .....	99
5.5	Kontrollgruppe: Datensparsamkeit .....	101
5.6	Kontrollgruppe: Datenübermittlung.....	102
5.7	Kontrollgruppe: Datenvorfall .....	104
5.7.1	Kontrolluntergruppe: Dokumentation .....	107
5.7.2	Kontrolluntergruppe: Mitteilungspflicht .....	108
5.8	Kontrollgruppe: Informationspflichten .....	113
5.8.1	Kontrolluntergruppe: Widerspruchsrecht .....	114
5.8.2	Kontrolluntergruppe: Datenverarbeitung .....	117
5.9	Kontrollgruppe: Rechtmäßigkeit .....	119
5.9.1	Kontrolluntergruppe: Prüfpflicht .....	120
5.10	Kontrollgruppe: Verantwortlichkeiten.....	120
5.10.1	Kontrolluntergruppe: Datenverarbeitung .....	121
5.10.2	Kontrolluntergruppe: Auftragsverarbeitung .....	122
<b>6.</b>	<b>Kontrollbereich Organisation .....</b>	<b>127</b>
6.1	Kontrollgruppe: Datenschutzkonzept und -management.....	127
6.1.1	Kontrolluntergruppe: Datenschutzbeauftragter.....	129
6.1.2	Kontrolluntergruppe: Leitende Organe.....	134
6.1.3	Kontrolluntergruppe: Risikobewertung.....	139
6.1.4	Kontrolluntergruppe: Verschwiegenheit .....	141
6.2	Kontrollgruppe: Verantwortlichkeiten.....	142
6.2.1	Kontrolluntergruppe: Datenverarbeitung .....	143
<b>7.</b>	<b>Kontrollbereich IT .....</b>	<b>145</b>
7.1	Kontrollgruppe: Betroffenenrechte .....	145
7.2	Kontrollgruppe: Aufbewahrung von Daten.....	146
7.2.1	Kontrolluntergruppe: Aufbewahrungszeiten.....	147
7.2.2	Kontrolluntergruppe: Sperr- und Löschkonzept.....	148
7.2.3	Kontrolluntergruppe: Protokollierung (Logdaten) .....	150
7.3	Kontrollgruppe: Datenschutzkonzept und -management.....	153
7.3.1	Kontrolluntergruppe: Richtlinien und Nachweise.....	153
7.4	Kontrollgruppe: Datensicherheitsmaßnahmen .....	154
7.4.1	Kontrolluntergruppe: Aufgabenzuordnung und Belehrung.....	156
7.4.2	Kontrolluntergruppe: Risikobewertung.....	156
7.4.3	Kontrolluntergruppe: Datenklassifikation .....	158
7.4.4	Kontrolluntergruppe: Zugriffskonzept .....	159
7.4.5	Kontrolluntergruppe: Netzwerksicherheit .....	165
7.4.6	Kontrolluntergruppe: Zutrittskonzept .....	166
7.4.7	Kontrolluntergruppe: Verfügbarkeit.....	169

7.4.8	Kontrolluntergruppe: Integrität .....	172
7.4.9	Kontrolluntergruppe: Belastbarkeit (Performance) .....	173
7.4.10	Kontrolluntergruppe: Kommunikationssicherheit .....	174
7.4.11	Kontrolluntergruppe: Protokollierung (Logging) .....	175
7.5	Kontrollgruppe: Datensparsamkeit .....	177
7.6	Kontrollgruppe: Datenübermittlung .....	179
7.7	Kontrollgruppe: Nationales Datenschutzrecht .....	182
8.	<b>Verhaltensregeln und Zertifizierungen</b> .....	185
8.1	ISAE 3000 .....	186
8.2	Das Europäische Datenschutz-Gütesiegel „EuroPriSe“ .....	188
8.3	ISO 27001 mit Schwerpunkt Datenschutz .....	189
	<b>Abbildungsverzeichnis</b> .....	191
	<b>Stichwortverzeichnis</b> .....	193