

Datenschutz-Audit

Recht – Organisation – Prozess – IT

Pachinger/Beham (Hrsg.)

HINWEIS/DISCLAIMER:

Die Aufbereitung der einzelnen Kontrollbereiche, Kontrollgruppen und Kontrollen basiert auf den bisherigen Erfahrungen der Herausgeber und Autoren bei der Durchführung von Datenschutz-Audits nach der aktuellen Rechtslage. Die Methodik wurde in Anlehnung an Audits von Managementsystemen entwickelt. Die aus den Verpflichtungen der DSGVO „abgeleiteten“ Kontrollen/Maßnahmen sind Möglichkeiten, die Erfüllung der Anforderungen der DSGVO und des BDSG nachzuweisen („Good Practice“). Keinesfalls wird damit gesagt, dass diese Kontrollen/Maßnahmen die ausschließlich relevanten bzw notwendigen sind, um die Erfüllung der Vorgaben der DSGVO und des DSGVO vollständig nachzuweisen; das vorliegende Werk stellt auch keine Rechts- oder Security-Beratung dar und ersetzt nicht die rechtliche Beratung im Einzelfall. Zu beachten ist daher, dass Datenschutz- und Aufsichtsbehörden oder auch Gerichte im Einzelfall andere oder weitere Nachweise verlangen können. Die Herausgeber und Autoren übernehmen daher keine Haftung für die korrekte Erfüllung von Vorgaben der DSGVO und des BDSG.

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

ISBN 978-3-8005-1798-5

dfv Mediengruppe



© 2022 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main
www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Druck: WIRMachenDRUCK GmbH, Backnang

Printed in Germany

Inhaltsverzeichnis

Vorwort der Herausgeber und Autoren	V
Vorwort von Jörg Asma	VII
Abkürzungsverzeichnis	XIII
Literaturverzeichnis	XV
Autorenverzeichnis	XIX
1. Einführung	1
1.1 Die Datenschutz-Grundverordnung (DSGVO)	3
1.2 Accountability als Grundlage verpflichtender Datenschutz-Audits	4
1.3 Das deutsche Datenschutzrecht	5
2. Grundlagen eines Audits	9
2.1 Einleitung	9
2.2 Begriffsdefinition	10
2.2.1 Handelnde Parteien eines Audits	10
2.2.2 Auditkriterien und -ergebnisse	12
2.2.2.1 Auditkriterien	12
2.2.2.2 Auditnachweise	12
2.2.2.3 Auditfeststellungen	12
2.2.2.4 Auditschlussfolgerung	13
2.2.3 Auditvarianten	13
2.3 Grundsätze eines Audits	14
2.4 Planung eines Audits	14
2.4.1 Auditprogramm	15
2.4.2 Zeitmanagement beim Audit	18
2.5 Auditablauf	20
2.5.1 Durchführen des Eröffnungsgespräches	20
2.5.2 Durchführen des Audits	21
2.5.3 Audittools	23
2.5.4 Kommunikation während des Audits	25
2.5.5 Abschlussgespräch	26
2.6 Auditbericht	27
2.7 Nachbearbeitung von Audits	28
3. Kontrollbereiche als Basis für das Datenschutz-Audit	29
3.1 Gliederung	29
3.1.1 Kontrollbereiche (Recht, Organisation, Prozess, IT – „ROPI“)	29
3.1.2 Verpflichtungen	29
	IX

Inhaltsverzeichnis

3.1.3	Kontrollen	30
3.1.4	Kontrollgruppen	30
3.1.5	Kontrolluntergruppen	31
3.2	Beschreibung der Kontrollgruppen	31
3.2.1	Kontrollgruppe: Anwendungsbereich DSGVO	31
3.2.2	Kontrollgruppe: Betroffenenrechte	31
3.2.3	Kontrollgruppe: Aufbewahrung von Daten	32
3.2.4	Kontrollgruppe: Datenschutz-Folgenabschätzung	32
3.2.5	Kontrollgruppe: Datenschutzkonzept und -management	33
3.2.6	Kontrollgruppe: Datensicherheitsmaßnahmen	33
3.2.7	Kontrollgruppe: Datensparsamkeit	33
3.2.8	Kontrollgruppe: Datenübermittlung	34
3.2.9	Kontrollgruppe: Datenvorfall	34
3.2.10	Kontrollgruppe: Informationspflichten	34
3.2.11	Kontrollgruppe: Rechtmäßigkeit	35
3.2.12	Kontrollgruppe: Verantwortlichkeiten	35
3.2.13	Kontrollgruppe: Nationales Datenschutzrecht	36
4.	Kontrollbereich Recht	37
4.1	Kontrollgruppe: Anwendungsbereich DSGVO	37
4.1.1	Kontrolluntergruppe: Datenklassifikation	38
4.2	Kontrollgruppe: Betroffenenrechte	40
4.3	Kontrollgruppe: Aufbewahrung von Daten	43
4.4	Kontrollgruppe: Datenschutz-Folgenabschätzung	44
4.4.1	Kontrolluntergruppe: Maßnahmen	48
4.5	Kontrollgruppe: Datenschutzkonzept und -management	52
4.6	Kontrollgruppe: Datenübermittlung	53
4.6.1	Kontrolluntergruppe: Zulässigkeit	55
4.7	Kontrollgruppe: Informationspflichten	61
4.7.1	Kontrolluntergruppe: Datenverarbeitung	62
4.7.2	Kontrolluntergruppe: Verfahren	63
4.8	Kontrollgruppe: Rechtmäßigkeit	64
4.8.1	Kontrolluntergruppe: Datenklassifikation	69
4.8.2	Kontrolluntergruppe: Einwilligung und weitere Rechtsgrundlagen	72
4.8.3	Kontrolluntergruppe: Prüfpflicht	77
4.8.4	Kontrolluntergruppe: Zweckbindung	80
4.9	Kontrollgruppe: Verantwortlichkeiten	80
4.9.1	Kontrolluntergruppe: Gemeinsame Datenverarbeitung	81
4.10	Kontrollgruppe: Nationales Datenschutzrecht	83
5.	Kontrollbereich Organisation	106
5.1	Kontrollgruppe: Datenschutzkonzept und -management	106

Inhaltsverzeichnis

5.1.1	Kontrolluntergruppe: Datenschutzbeauftragter	108
5.1.2	Kontrolluntergruppe: Leitende Organe	114
5.1.3	Kontrolluntergruppe: Risikobewertung	120
5.1.4	Kontrolluntergruppe: Verschwiegenheit	123
5.2	Kontrollgruppe: Verantwortlichkeiten	124
5.2.1	Kontrolluntergruppe: Datenverarbeitung	125
5.3	Kontrollgruppe: Nationales Datenschutzrecht	126
6.	Kontrollbereich Prozess	129
6.1	Kontrollgruppe: Anwendungsbereich DSGVO	129
6.1.1	Kontrolluntergruppe: Datenklassifikation	130
6.2	Kontrollgruppe: Betroffenenrechte	132
6.2.1	Kontrolluntergruppe: Datensparsamkeit	136
6.2.2	Kontrolluntergruppe: Informationspflicht	137
6.2.3	Kontrolluntergruppe: Löschung	143
6.2.4	Kontrolluntergruppe: Richtigstellung	148
6.2.5	Kontrolluntergruppe: Widerspruch	151
6.3	Kontrollgruppe: Aufbewahrung von Daten	152
6.4	Kontrollgruppe: Datenschutzkonzept und -management	152
6.4.1	Kontrolluntergruppe: Dokumentation und Nachweise ..	153
6.5	Kontrollgruppe: Datensparsamkeit	156
6.6	Kontrollgruppe: Datenübermittlung	157
6.7	Kontrollgruppe: Datenvorfall	160
6.7.1	Kontrolluntergruppe: Dokumentation	162
6.7.2	Kontrolluntergruppe: Mitteilungspflicht	164
6.8	Kontrollgruppe: Informationspflichten	170
6.8.1	Kontrolluntergruppe: Widerspruchsrecht	172
6.8.2	Kontrolluntergruppe: Datenverarbeitung	174
6.9	Kontrollgruppe: Rechtmäßigkeit	178
6.9.1	Kontrolluntergruppe: Prüfpflicht	178
6.10	Kontrollgruppe: Verantwortlichkeiten	179
6.10.1	Kontrolluntergruppe: Datenverarbeitung	180
6.10.2	Kontrolluntergruppe: Auftragsverarbeitung	181
6.11	Kontrollgruppe: Nationales Datenschutzrecht	185
7.	Kontrollbereich IT	187
7.1	Kontrollgruppe: Betroffenenrechte	187
7.2	Kontrollgruppe: Aufbewahrung von Daten	188
7.2.1	Kontrolluntergruppe: Aufbewahrungszeiten	189
7.2.2	Kontrolluntergruppe: Sperr- und Löschkonzept	191
7.2.3	Kontrolluntergruppe: Protokollierung (Logdaten)	193
7.3	Kontrollgruppe: Datenschutzkonzept und -management	196
7.3.1	Kontrolluntergruppe: Richtlinien und Nachweise	197

Inhaltsverzeichnis

7.4	Kontrollgruppe: Datensicherheitsmaßnahmen	198
7.4.1	Kontrolluntergruppe: Aufgabenzuordnung und Belehrung 200	
7.4.2	Kontrolluntergruppe: Risikobewertung	200
7.4.3	Kontrolluntergruppe: Datenklassifikation	202
7.4.4	Kontrolluntergruppe: Zugriffskonzept	204
7.4.5	Kontrolluntergruppe: Netzwerksicherheit	211
7.4.6	Kontrolluntergruppe: Zutrittskonzept	213
7.4.7	Kontrolluntergruppe: Verfügbarkeit	215
7.4.8	Kontrolluntergruppe: Integrität	219
7.4.9	Kontrolluntergruppe: Belastbarkeit (Performance)	220
7.4.10	Kontrolluntergruppe: Kommunikationssicherheit	221
7.4.11	Kontrolluntergruppe: Protokollierung (Logging)	222
7.5	Kontrollgruppe: Datensparsamkeit	225
7.6	Kontrollgruppe: Datenübermittlung	227
7.7	Kontrollgruppe: Nationales Datenschutzrecht	231
8.	Verhaltensregeln und Zertifizierungen	233
8.1	ISAE 3000	234
8.2	Das Europäische Datenschutz-Gütesiegel „EuroPriSe“	237
8.3	ISO 27001	238
8.4	ISO 27701 Sicherheitsverfahren – Erweiterung zu ISO/ IEC 27001 und ISO/IEC 27002 für das Datenschutzmanage- ment – Anforderungen und Leitfaden	239
8.5	ISO 27017 Datensicherheit in der Cloud	240
8.6	ISO 27018 Datenschutz und Datensicherheit in der Cloud	241
8.7	Nationale Zertifizierungen und Testate	242
8.7.1	IT-Grundschutz	242
8.7.1	Attestierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)	243
9.	Entscheidungen – Geldbußen nach der DSGVO	244
	Abbildungsverzeichnis	250
	Stichwortverzeichnis	251