

**Vorgehen und Prüfpunkte für ein  
Datenschutzaudit gemäß  
DGI-DSM:2020-05**

**- Richtlinie -**

## Inhaltsverzeichnis

Prüfung und Freigabe .....	2
Änderungshistorie.....	3
Dokumentensteuerung und Verteilerkreis .....	4
1 Angaben zum Audit .....	7
2 Festlegungen zum Audit.....	8
2.1 Auditkriterien .....	8
2.2 Auditprüfpunkte.....	8
2.3 Festlegung der Prüfkriterien.....	9
2.4 Festlegung der Bewertungskriterien .....	9
3 Hinweise für den Umgang mit der Auditcheckliste .....	10
3.1 Allgemeines .....	10
3.2 Umgang mit den Auditfeststellungen .....	10
4 Prüfpunkte .....	12
4.1 Allgemeines .....	12
4.2 Prüfpunkte gemäß DGI-DSM:2020-05 .....	12
Einhaltung von geeigneten technischen und organisatorischen Maßnahmen (TOM).....	12
Einhaltung von geeigneten technischen und organisatorischen Maßnahmen (TOM).....	13
Initiierung und Umsetzung eines Datenschutzmanagementsystems (DSMS) .....	14
Initiierung und Umsetzung eines Datenschutzmanagementsystems (DSMS) .....	15
Benennung eines Datenschutzbeauftragten (DSB) gemäß Artikel 37.....	16
Kommunikation der Benennung des Datenschutzbeauftragten gemäß Artikel 37 .....	17
Darstellung des Datenschutzbeauftragten in der Aufbauorganisation gemäß Artikel 38 .....	18
Benennung und Herausstellung der Ansprechpartner und Koordinatoren gemäß Artikel 39.....	19
Eruierung aller datenschutzrechtlichen Anforderungen aus der Compliance gemäß Artikel 39 Absatz 1 Buchstabe b .....	20
Erstellung und Veröffentlichung einer Leitlinie zum Datenschutz gemäß Artikel 24 .....	21
Erstellung und Veröffentlichung einer Leitlinie zum Datenschutz gemäß Artikel 24 .....	22
Unterweisung aller Beschäftigten zu Themen des Datenschutzes gemäß Artikel 29 und Artikel 32 Absatz 4.....	23
Verpflichtung aller Beschäftigten auf das Datengeheimnis gemäß Artikel 29 und Artikel 32 Absatz 4 24	
Ordnungsgemäße und frühzeitige Einbindung des Datenschutzbeauftragten gemäß Artikel 38.....	25
Eruierung der Notwendigkeit einer Datenschutzfolgenabschätzung (DSFA) gemäß Artikel 35.....	26
Durchführung einer Datenschutzfolgenabschätzung (DSFA) gemäß Artikel 35.....	27
Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten gemäß Artikel 30.....	28
Einhaltung der Grundsätze der Verarbeitung von pbDaten gemäß Artikel 5.....	29
Einhaltung der Informationspflichten gemäß Artikel 13 und Artikel 14 .....	30
Einhaltung der Auskunftsrechte der betroffenen Person gemäß Artikel 15.....	31
Einhaltung des Rechts auf Berichtigung oder Vervollständigung gemäß Artikel 16.....	32
Einhaltung des Rechts auf Berichtigung oder Vervollständigung gemäß Artikel 16.....	33

---

Einhaltung des Rechts auf Löschung gemäß Artikel 17 .....	34
Einhaltung des Rechts auf Löschung gemäß Artikel 17 .....	35
Einhaltung des Rechts auf Einschränkung der Verarbeitung gemäß Artikel 18 .....	36
Einhaltung des Rechts auf Einschränkung der Verarbeitung gemäß Artikel 18 .....	37
Einhaltung des Rechts auf Datenübertragbarkeit gemäß Artikel 20 .....	38
Einhaltung des Widerspruchsrechts gemäß Artikel 21 .....	39
Einhaltung des Widerspruchsrechts gemäß Artikel 21 .....	40
Steuerung von Auftragsverarbeitern gemäß Artikel 28 .....	41
Eruierung der Datenübermittlung an unsichere Drittländer gemäß Artikel 44 .....	42
Einhaltung der Meldung von Verletzungen des Schutzes von pbDaten gemäß Artikel 33 .....	43

Bitte dieses Dokument an Ihre Organisation anpassen