Muster-Prüfprogramm

Datenschutz

Technisch-organisatorische Maßnahmen

12 Prüfschritte · DSGVO

12 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

DSGVO Art. 32(1) und (2) · DSGVO Art. 32(1) · DSGVO Art. 32(1)(a) · DSGVO Art. 32(1)(b) · ISO/IEC 27001:2022 Anhang A 5.15 · ISO/IEC 27001:2022 Anhang A 8.15 · BSI OPS.1.1.4 · DSGVO Art. 32(1)(c) · DSGVO Art. 32(1)(d) · DSGVO Art. 32(4) · DSGVO Art. 28(1) und (3) · DSGVO Art. 28(3)(h) · DSGVO Art. 33(1) und (5)

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob Verantwortliche und Auftragsverarbeiter ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten gewährleisten: Risikobetrachtung, Verschlüsselung und Pseudonymisierung, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, Wiederherstellung nach Störungen und regelmäßige Überprüfung. Sie beurteilt außerdem, ob Beschäftigte nur auf Weisung mit Daten umgehen und ob Auftragsverarbeiter eingebunden sind.

GELTUNGSBEREICH

- Verarbeitungstätigkeiten mit personenbezogenen Daten, ausgewählt nach Risiko, und die dafür eingesetzten Systeme
- Technische Maßnahmen wie Verschlüsselung, Zugriffsschutz, Datensicherung und Protokollierung
- Organisatorische Maßnahmen wie Richtlinien, Schulung, Verpflichtungen und Prozesse für Vorfälle
- Nicht Gegenstand: Rechtmäßigkeit der Verarbeitung, Betroffenenrechte und Datenübermittlung in Drittländer, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01 — DSGVO Art. 32(1) und (2)

Das Risiko für die Rechte und Freiheiten betroffener Personen wird für die Verarbeitungstätigkeiten bewertet, die Bewertung berücksichtigt Eintrittswahrscheinlichkeit und Schwere und ist aktuell.

Prüfhandlung Für fünf Verarbeitungstätigkeiten die Risikobewertung ansehen und ihre Aktualität sowie die Herleitung des Schutzniveaus prüfen.

Nachweise Verzeichnis der Verarbeitungstätigkeiten, Risikobewertungen

Schritt 02 — DSGVO Art. 32(1)

Die Maßnahmen sind dokumentiert und stehen in angemessenem Verhältnis zum Risiko, Stand der Technik und Implementierungskosten sind berücksichtigt.

Prüfhandlung Maßnahmenkatalog lesen und für drei Verarbeitungstätigkeiten die Zuordnung der Maßnahmen zum Risiko nachvollziehen.

Nachweise Maßnahmenkonzept, Zuordnung von Risiko und Maßnahme

Schritt 03 — DSGVO Art. 32(1)(a)

Personenbezogene Daten werden, wo angemessen, verschlüsselt oder pseudonymisiert, bei Speicherung und Übertragung.

Prüfhandlung Verschlüsselungseinstellungen für Datenbanken, Datensicherungen, mobile Geräte und Übertragungswege einer Stichprobe prüfen.

Nachweise Konfigurationsauszüge, Konzept zu Verschlüsselung und Pseudonymisierung

Prüfschritte 4 bis 6

Schritt 04 DSGVO Art. 32(1)(b); ISO/IEC 27001:2022 Anhang A 5.15

Die Vertraulichkeit wird durch ein Berechtigungskonzept gesichert: Zugriff nur für Befugte, nach Erforderlichkeit, mit regelmäßiger Überprüfung.

Prüfhandlung Berechtigungen auf Systemen mit personenbezogenen Daten mit dem Konzept abgleichen und die letzte Überprüfung ansehen.

Nachweise Berechtigungskonzept, Rechteauszüge, Überprüfungsprotokoll

Schritt 05 DSGVO Art. 32(1)(b); ISO/IEC 27001:2022 Anhang A 8.15

Integrität der Daten und Systeme wird gesichert, etwa durch Änderungsschutz, Protokollierung und Prüfung auf unbefugte Veränderung.

Prüfhandlung Protokollierung von Änderungen an Datenbeständen und Schutz der Protokolle in zwei Systemen prüfen.

Nachweise Protokollkonfiguration, Auswertungen

Schritt 06 DSGVO Art. 32(1)(b); BSI OPS.1.1.4

Verfügbarkeit und Belastbarkeit der Systeme sind durch Redundanz, Kapazitätsplanung und Schutz vor Schadsoftware gesichert.

Prüfhandlung Verfügbarkeitsanforderungen mit der technischen Umsetzung vergleichen und die Abdeckung des Schutzes vor Schadsoftware prüfen.

Nachweise Architekturübersicht, Verfügbarkeitsberichte, Abdeckung der Schutzsoftware

Prüfschritte 7 bis 9

Schritt 07 — DSGVO Art. 32(1)(c)

Nach einem physischen oder technischen Zwischenfall können Verfügbarkeit und Zugang zu den Daten rasch wiederhergestellt werden; die Wiederherstellung wird getestet.

Prüfhandlung Datensicherungs- und Wiederherstellungskonzept lesen und die Ergebnisse des letzten Wiederherstellungstests ansehen.

Nachweise Sicherungskonzept, Protokoll des Wiederherstellungstests

Schritt 08 — DSGVO Art. 32(1)(d)

Die Wirksamkeit der Maßnahmen wird in einem festgelegten Verfahren regelmäßig überprüft, bewertet und evaluiert; Ergebnisse führen zu Maßnahmen.

Prüfhandlung Prüfplan und Berichte der letzten zwölf Monate ansehen und die Umsetzung der Maßnahmen verfolgen.

Nachweise Prüfplan, Berichte interner und externer Prüfungen, Maßnahmenliste

Schritt 09 — DSGVO Art. 32(4)

Personen, die Zugang zu personenbezogenen Daten haben, verarbeiten sie nur auf Weisung und sind zur Vertraulichkeit verpflichtet und geschult.

Prüfhandlung Verpflichtungserklärungen und Schulungsnachweise einer Stichprobe von Beschäftigten prüfen.

Nachweise Verpflichtungserklärungen, Schulungsnachweise, Weisungen

Prüfschritte 10 bis 12

Schritt 10 — DSGVO Art. 28(1) und (3)

Mit Auftragsverarbeitern bestehen Verträge, die technische und organisatorische Maßnahmen, Weisungsbindung, Unterauftragsverhältnisse und Kontrollrechte regeln.

Prüfhandlung Verträge von drei Auftragsverarbeitern anhand einer Checkliste durchsehen und die Anlagen zu den Maßnahmen mit der Praxis abgleichen.

Nachweise Verträge zur Auftragsverarbeitung, Anlagen zu Maßnahmen, Checkliste

Schritt 11 — DSGVO Art. 28(3)(h)

Die Einhaltung durch Auftragsverarbeiter wird kontrolliert, etwa anhand von Nachweisen oder Prüfungen.

Prüfhandlung Nachweise und Kontrollen der letzten zwölf Monate für wesentliche Auftragsverarbeiter ansehen.

Nachweise Zertifikate, Prüfberichte, Protokolle von Kontrollen

Schritt 12 — DSGVO Art. 33(1) und (5)

Verletzungen des Schutzes personenbezogener Daten werden erkannt, dokumentiert und fristgerecht bewertet und gemeldet.

Prüfhandlung Verfahren zu Datenpannen prüfen und Dokumentation sowie Meldungen der letzten zwölf Monate ansehen.

Nachweise Verfahren, Dokumentation der Verletzungen, Meldungen

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Verzeichnis der Verarbeitungstätigkeiten
2. Risikobewertungen zu den Verarbeitungstätigkeiten der Stichprobe
3. Maßnahmenkonzept mit Zuordnung zum Risiko
4. Berechtigungskonzept und Rechteauszüge
5. Verschlüsselungs- und Pseudonymisierungskonzept
6. Sicherungskonzept und Protokoll des letzten Wiederherstellungstests
7. Verträge zur Auftragsverarbeitung mit Anlagen
8. Prüfpläne und Berichte der Überprüfung der Maßnahmen

TYPISCHE FESTSTELLUNGEN

- Die Maßnahmen sind nicht an das Risiko der Verarbeitungstätigkeit angebunden, es gibt ein Standardpaket für alle.
- Das Berechtigungskonzept ist nicht umgesetzt, auf Datenbestände mit personenbezogenen Daten greifen zu viele Personen zu.
- Datensicherungen sind nicht verschlüsselt, Wiederherstellungstests fehlen.
- Die Wirksamkeit der Maßnahmen wird nicht regelmäßig überprüft.
- Anlagen zu den technischen und organisatorischen Maßnahmen bei Auftragsverarbeitern sind veraltet oder allgemein gehalten.
- Beschäftigte sind nicht nachweislich verpflichtet und geschult.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026