Technische und organisatorische Maßnahmen (TOM) von dilohver

Technische und organisatorische Maßnahmen (TOM) sind zentral für die Datenschutzpraxis. Sie beschreiben Maßnahmen, die in erster Linie zum Schutz der verarbeiteten Daten ergriffen werden. Unterschieden werden technische Maßnahmen, die physisch umsetzbar sind, von organisatorischen Maßnahmen, die Verfahren, Abläufe und Handlungsanweisungen betreffen. Für diese TOM definiert das Standard-Datenschutz-Modell der deutschen Aufsichtsbehörden sieben Gewährleistungsziele.

Die Checkliste zeigt übersichtlich eine Auswahl von Maßnahmen nach dem Standard-Datenschutz-Modell (SDM) auf:

- Maßnahmen zur Datenminimierung, wie z. B. die Implementierung von Sperr- und Löschroutinen
- Maßnahmen zur Transparenz, wie z. B. die Protokollierung von Zugriffen und Änderungen
- Maßnahmen zur Intervenierbarkeit, wie z. B. die Einrichtung einer Deaktivierungsmöglichkeit für einzelne Funktionalitäten

Inhaltsverzeichnis

1.0 Vertraulichkeit

1.1 Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Besucher in Begleitung
Sicherheitsschlösser	Sorgfalt bei Auswahl Reinigungsdienst
	Clean-Desk-Policy
	Kein Papier im Büro (Hinweis: digitaler Dienstleister)

1.2 Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
2-Faktor-Identifiifiezierung	Erstellen von Benutzerprofilen
2 Fach Login mit unterschiedlichem Passwort zum Zugang auf unseren Server	Zentrale Passwortvergabe
Anti-Viren-Software Laptops	Richtlinie „Sicheres Passwort“
Anti-Viren-Software Geschäftshandys	Richtlinie „Sicheres Passwort“
Firewall	Richtlinie „Löschen / Vernichten“
Mobile Device Management	Richtlinie „Clean- Desk“
Einsatz VPN bei Remote-Zugriffen	Allg. Richtlinie Datenschutz und / oder Sicherheit
Verschlüsselung von Datenträgern	Mobile Device Policy
Verschlüsselung Smartphones	Anleitung „Manuelle Desktopsperre“
Gehäuseverriegelung	
BIOS Schutz (separates Passwort)	
Sperre externer Schnittstellen (USB)	
Automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablet	

1.3 Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte
Externer Aktenvernichter (DIN 32757)	Minimale Anzahl an Administratoren
Physische Löschung von Datenträgern	Datenschutztresor
	Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Festlegung von Datenbankrechten
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Datensätze sind mit Zweckattributen versehen

1.5 Pseudonymisierung

Technische Maßnahmen	Organisatorische Maßnahmen
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

2.0 Integrität

2.1 Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
E-Mail-Verschlüsselung	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Einsatz von VPN	Weitergabe in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter	Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
Bereitstellung über verschlüsselte Verbindungen wie z.B.: sftp, https	

2.2 Eingangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen

3.0 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	➔ Mit Sorgfalt ausgewählter externer Server ➔ regelmäßige Tests zur Datenwiederherstellung ➔ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

4.0 Verfügbarkeit und Belastbarkeit

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	Die Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)

4.2 Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind.	-
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	-

4.4 Auftragskontrolle (Outsourcing an Dritte)

Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.