

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO · [\[Firmenname\]](#) · Stand: [\[Datum\]](#) · GRATIS-VORLAGE

1. Allgemeines

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die [\[Firmenname\]](#) zum Schutz personenbezogener Daten gemäß Art. 32 DSGVO umsetzt. Es dient als Nachweis gegenüber Aufsichtsbehörden, Betroffenen und Auftraggebern (Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Je nach konkreter Verarbeitung und Rollenverteilung kann es als Anlage eines Auftragsverarbeitungsvertrags verwendet werden.

2. Maßnahmenkatalog (Auszug)

KATEGORIE	MASSNAHME	UMGESETZT
Zutrittskontrolle	Abschließbare Büro-/Serverräume, Schlüsselverwaltung	☐
	Besucherregelung mit Begleitung	☐
Zugangskontrolle	Passwort-Richtlinie (Mindestlänge [12] Zeichen)	☐
	Multi-Faktor-Authentifizierung für alle Systeme mit Personenbezug	☐
	Automatische Bildschirmsperre nach [5] Minuten	☐
Zugriffskontrolle	Berechtigungskonzept nach Least-Privilege-Prinzip	☐
	Protokollierung von Zugriffen auf personenbezogene Daten	☐
Verfügbarkeit	Backup-Konzept (3-2-1-Regel), regelmäßige Wiederherstellungstests	☐
	Aktuelle Virenschutz-/EDR-Lösung, zeitnahes Patch-Management	☐
Verschlüsselung	Datenträgerverschlüsselung, TLS für Übertragungen	☐
Auftragskontrolle	AVV mit allen Auftragsverarbeitern (Art. 28 DSGVO)	☐
Trennungskontrolle	Getrennte Verarbeitung unterschiedlicher Zwecke, Mandantentrennung	☐
Organisation	Datenschutzschulungen ([jährlich]), Verpflichtung der Beschäftigten	☐
Incident Response	Prüf- und Meldeprozess für Datenschutzverletzungen; bei voraussichtlichem Risiko Meldung an die Aufsichtsbehörde möglichst binnen 72 Stunden nach Bekanntwerden (Art. 33 DSGVO)	☐

3. Überprüfung

Die Wirksamkeit der Maßnahmen wird [\[jährlich\]](#) überprüft (Art. 32 Abs. 1 lit. d DSGVO).
Verantwortlich: [\[Name\]](#). Letzte Überprüfung: [\[Datum\]](#).

Dies ist die kostenlose Kurzversion. Die Vollversion umfasst 25 Kapitel mit vollständigen Maßnahmenkatalogen in drei Schutzniveaus (Basis/Standard/Hoch), Schutzbedarfsklassifizierung, NIS2-Bezügen, Drittland-Kapitel und Freigabe-Block - per Assistent auf Ihre IT-Landschaft zugeschnitten, mit 9 weiteren Pflichtdokumenten. SecKit · 149 € einmalig · magra-sec.de/seckit
Mustervorlage, keine Rechtsberatung. Rechtsstand: Juli 2026. © MAGRA SEC