tribeta

WHITEPAPER · DATENSCHUTZ

TOMs richtig umsetzen

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO strukturiert planen, umsetzen und nachweisen.

DSGVO Art. 32 | BDSG | Ausgabe 2026

tribeta GmbH i.G. · tribeta-group.de · Poststr. 67, 53840 Troisdorf

INHALT

MANAGEMENT SUMMARY

Das Wichtigste in Kürze

Technische und organisatorische Maßnahmen (TOMs) sind das Herzstück der Datensicherheit nach der DSGVO. Artikel 32 verpflichtet jedes Unternehmen, ein dem Risiko **angemessenes Schutzniveau** für personenbezogene Daten sicherzustellen — und dies nachweisen zu können.

Dieses Whitepaper erklärt, was TOMs sind, wie Sie sie **risikobasiert** auswählen, welche Maßnahmen-Kategorien relevant sind und wie Sie alles revisionssicher dokumentieren.

01 Was TOMs sind und warum sie Pflicht sind

TOMs sind alle Vorkehrungen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Daten gewährleisten. Die DSGVO nennt sie in Art. 32 (Sicherheit der Verarbeitung) und macht sie für Verantwortliche und Auftragsverarbeiter gleichermaßen verbindlich.

Weil die **Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO) gilt, reicht es nicht, Maßnahmen umzusetzen — Sie müssen sie auch belegen können. Fehlende oder unzureichende TOMs sind ein häufiger Anlass für Bußgelder.

20 Mio. €
oder 4 % des Jahresumsatzes — max. Bußgeld

Art. 32
Sicherheit der Verarbeitung

Angemessen, nicht maximal

Gefordert ist ein zum Risiko passendes Schutzniveau — unter Berücksichtigung von Stand der Technik, Umsetzungskosten sowie Art, Umfang und Zweck der Verarbeitung.

02 Der risikobasierte Ansatz

Die DSGVO schreibt keinen festen Maßnahmenkatalog vor. Stattdessen ermitteln Sie den **Schutzbedarf** je Verarbeitung und leiten daraus passende Maßnahmen ab. Grundlage ist eine Einschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden für die betroffenen Personen.

- **Schutzbedarf bestimmen** — normal, hoch oder sehr hoch, je nach Sensibilität der Daten.
- **Risiken bewerten** — Wahrscheinlichkeit und mögliche Auswirkungen abwägen.
- **Maßnahmen zuordnen** — Stand der Technik und Verhältnismäßigkeit beachten.
- **Wirksamkeit prüfen** — regelmäßig evaluieren und aktualisieren.

> KERNAUSSAGE
>
> Nicht jede Maßnahme ist für jeden Pflicht — die Angemessenheit richtet sich nach dem konkreten Risiko der Verarbeitung.

03 Die zentralen Maßnahmen-Kategorien

In der Praxis haben sich Kontrollziele bewährt, die den gesamten Datenlebenszyklus abdecken. Sie helfen, keine Lücke zu übersehen:

- **Zutritts- und Zugangskontrolle** — physischer Schutz von Räumen und Systemen, Authentifizierung.
- **Zugriffskontrolle** — Berechtigungskonzept nach dem Need-to-know-Prinzip.
- **Weitergabe- und Eingabekontrolle** — verschlüsselte Übertragung, Protokollierung.
- **Pseudonymisierung und Verschlüsselung** — Art. 32 nennt sie ausdrücklich.
- **Verfügbarkeit und Belastbarkeit** — Backups, Redundanz, Notfallkonzept.
- **Auftrags- und Trennungskontrolle** — AV-Verträge, getrennte Verarbeitung.
- **Verfahren zur Überprüfung** — regelmäßige Evaluierung der Wirksamkeit.

04 Dokumentation und Nachweis

Ein **TOM-Konzept** fasst Ihre Maßnahmen strukturiert zusammen und ist zugleich Anlage zu Auftragsverarbeitungsverträgen. Es verknüpft jede Maßnahme mit dem adressierten Risiko und dem Verantwortlichen.

Praxistipp

Verweisen Sie im Verzeichnis der Verarbeitungstätigkeiten (Art. 30) auf Ihr TOM-Konzept und halten Sie beide synchron — so entsteht ein lückenloser Nachweis.

05 Typische Fehler vermeiden

- TOMs einmalig erstellen und nie wieder aktualisieren.
- Standardlisten übernehmen, ohne den eigenen Risikokontext zu prüfen.
- Verschlüsselung und Löschkonzept vernachlässigen.
- Dienstleister ohne AV-Vertrag und ohne Prüfung ihrer TOMs einsetzen.
- Wirksamkeit nie messen — Maßnahmen bleiben auf dem Papier.

QUELLEN & RECHTSGRUNDLAGEN

DSGVO — Verordnung (EU) 2016/679, insb. Art. 5 Abs. 2, Art. 24, Art. 32; Bundesdatenschutzgesetz (BDSG); BSI IT-Grundschutz; Leitlinien des Europäischen Datenschutzausschusses (EDSA). Stand 2026.