

# TOM-Checkliste

Technische und organisatorische Maßnahmen überprüfen



Vorausgefüllte Vorlagen vom  
Datenschutz-Auditor (TÜV-geprüft)

- 📁 Offline Datenschutz-Managementsystem nach DSGVO:  
Direkt-Download in Excel oder Word.
- ✓ Verzeichnis von Verarbeitungstätigkeiten, TOM,  
Schulung, Auditcheckliste, Datenschutzkonzept,  
Risikoanalyse uvm.
- € Sparen Sie tausende Euro Beratungsgebühren und  
tagelange Recherche

**Jetzt informieren!**

Eine weitere Checkliste für die gesamte DSGVO gibt es **kostenlos** unter:

<https://dsgvo-vorlagen.de/dsgvo-checkliste-beratung>

## Checkliste

- Existiert überhaupt eine Dokumentation zu allen umgesetzten TOM?

**Praxisbeispiel:** Eine Excel Tabelle, in der alle Bestandteile der TOM in einer Liste dargestellt sind.

Kommentare

- Existiert ein Löschkonzept und wird dies für alle personenbezogenen Daten umgesetzt?

**Praxisbeispiel:** Eine Excel Tabelle in der alle verarbeiteten Datenkategorien verzeichnet sind inkl. Löschrufen. Erstellung von Löschrufenprotokollen oder sonstigen Nachweisen.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung der Zutrittskontrolle dokumentiert und durchgeführt?

**Praxisbeispiel:** Alarmanlagen, Schließsysteme.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung der Zugangskontrolle dokumentiert und durchgeführt?

**Praxisbeispiel:** Installation einer Firewall, Verschlüsselung von Datenträgern.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung der Zugriffskontrolle dokumentiert und durchgeführt?

**Praxisbeispiel:** Passworrichtlinien, Löschanweisungen.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung der Weitergabekontrolle dokumentiert und durchgeführt?

**Praxisbeispiel:** E-Mail Verschlüsselung, Einsatz von VPN Technologie.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung der Eingabekontrolle dokumentiert und durchgeführt?

**Praxisbeispiel:** Eingabeprotokollierung, Nutzerrollen.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung der Verfügbarkeitskontrolle dokumentiert und durchgeführt?

**Praxisbeispiel:** Feuer- und Rauchmelder, automatische Löschanlagen.

Kommentare

- Wurden alle Maßnahmen zur Umsetzung des Trennungsgebots dokumentiert und durchgeführt?

**Praxisbeispiel:** Physische Trennung von Datenträgern, Speicherung von personenbezogenen Daten je nach Zweck in unterschiedlichen Datenbanken.

Kommentare

- Prüfen Sie alle Ihre Auftragsverarbeiter hinsichtlich der Einhaltung der Datenschutzgrundsätze?

**Praxisbeispiel:** Vorabkontrolle beim Auftragsverarbeiter, Prüfung der TOMs des Auftragsverarbeiters.

Kommentare

- Bestehen Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall?

**Praxisbeispiel:** Backups, Incident Response Management.

Kommentare

- Gibt es Vertretungsregelungen für die IT-Verantwortlichen?

**Praxisbeispiel:** Wenn der IT-Leiter krank ist, kann der stellvertretende IT-Leiter seine Aufgaben übernehmen.

Kommentare

- Sind die Verantwortlichen für die IT-Sicherheit angemessen ausgebildet und in alle Unternehmensstrukturen eingebunden, die mit personenbezogenen Daten zu tun haben?

**Praxisbeispiel:** Der IT-Sicherheitsbeauftragte des Unternehmens wird bei jeder Tool-Neuanschaffung mit eingebunden.

Kommentare

- Existieren Verfahren zur Gewährleistung der Belastbarkeit der Systeme und Dienste?

**Praxisbeispiel:** Regelmäßige Tests der Belastbarkeit mittels Stresstests.

Kommentare

- Existiert ein Datensicherheitskonzept bzw. eine Datensicherheitsrichtlinie?

**Praxisbeispiel:** Ausarbeitung einer Datensicherheitsrichtlinie mit einem Berater.

Kommentare

- Wurden alle Mitarbeiter, die mit personenbezogenen Daten zu tun haben, auf das Datengeheimnis verpflichtet und wurden im Umgang mit den Daten geschult?

**Praxisbeispiel:** Aushändigung einer Schulungsunterlage im Jahresrhythmus, Verpflichtung aller Mitarbeiter auf das Datengeheimnis mit Unterschrift.

Kommentare



**Vorausgefüllte Vorlagen vom  
Datenschutz-Auditor (TÜV-geprüft)**

-  Offline Datenschutz-Managementsystem nach DSGVO:  
Direkt-Download in Excel oder Word.
-  Verzeichnis von Verarbeitungstätigkeiten, TOM,  
Schulung, Auditcheckliste, Datenschutzkonzept,  
Risikoanalyse uvm.
-  Sparen Sie tausende Euro Beratungsgebühren und  
tagelange Recherche

[Jetzt informieren!](#)

- Existieren Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen?

**Praxisbeispiel:** Die TOMs werden jedes Jahr unabhängig geprüft, die Prüfung und die Findings werden dokumentiert.

Kommentare

- Entsprechen die TOM dem aktuellen Stand des technischen Fortschritts und sind gemäß festgelegten Schutzziele und Risikoprofil angemessen?

Kommentare