

TOM-Checkliste

Technische & organisatorische Maßnahmen · Art. 32 DSGVO · Vorlage für KMU

Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E) · Bereitgestellt von ETHYX · Version 1.1 · Juli 2026 · Keine Rechtsberatung

HINWEIS Arbeiten Sie jeden Abschnitt durch und setzen Sie das Häkchen, wenn eine Maßnahme umgesetzt ist. Nutzen Sie Status / Notizen für Teilumsetzung, die verantwortliche Person oder das System – vermerken Sie 'Entfällt' mit kurzer Begründung, wo eine Maßnahme nicht zutrifft. Mindestens jährlich überprüfen. Die §-Nummern entsprechen den TOM-Verweisen in der ETHYX-VVT-Vorlage.

**Unternehmen /
Verantwortlicher:**

Ausgefüllt von:

Nächste Prüfung:

Datum:

Worum es geht

Art. 32 DSGVO verpflichtet jeden Verantwortlichen und Auftragsverarbeiter, geeignete technische und organisatorische Maßnahmen (TOM) zum Schutz personenbezogener Daten umzusetzen. Diese Checkliste dokumentiert sie – die Sicherheitsanlage, auf die Ihre AVV und Ihr VVT verweisen, und das erste Dokument, das eine Behörde oder ein Unternehmenskunde anfragt.

§1 Zutrittskontrolle

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Server und IT-Geräte befinden sich in abschließbaren Räumen mit beschränktem Zugang.	
☐	Ein Zutrittssystem (Schlüssel, Karten oder Codes) regelt den Zugang; die Ausgabe ist dokumentiert.	
☐	Besucher werden erfasst und in Bereichen mit Datenverarbeitung begleitet.	
☐	Die Räumlichkeiten sind gesichert (Alarmanlage, Schlösser und/oder Sicherheitsdienst nach Bedarf).	
☐	Es gilt eine Clean-Desk-Richtlinie; Papierunterlagen werden in abschließbaren Schränken aufbewahrt.	
☐	Papier wird nach DIN 66399 vernichtet; Datenträger werden vor Entsorgung sicher gelöscht oder zerstört.	
☐	Cloud/Remote: Die physische Sicherheit liegt beim Hosting-/Rechenzentrumsanbieter – Zertifizierung (z. B. ISO 27001) prüfen und im AVV festhalten.	

§2**Zugangs- & Zugriffskontrolle**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Jeder Nutzer hat ein eindeutiges persönliches Konto; gemeinsame Logins werden nicht verwendet.	
☐	Eine Passwortrichtlinie wird durchgesetzt (Mindestlänge, Komplexität, keine kompromittierten Passwörter).	
☐	Multi-Faktor-Authentifizierung (MFA) ist für kritische Systeme und jeden Fernzugriff erforderlich.	
☐	Der Zugriff folgt dem Least-Privilege-/Rollenprinzip; eine Berechtigungsmatrix ist dokumentiert und wird geprüft.	
☐	Bildschirme sperren automatisch bei Inaktivität; Sitzungen laufen ab.	
☐	Beim Ausscheiden oder Rollenwechsel werden Berechtigungen unverzüglich entzogen (Offboarding-Checkliste).	
☐	Zugriffe auf Systeme mit personenbezogenen Daten werden protokolliert.	
☐	Laptops und Mobilgeräte werden verwaltet (MDM) und sind verschlüsselt.	

§3**Netzwerk- & Serversicherheit**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Eine Firewall schützt das Netzwerk; eine Segmentierung trennt sensible Systeme.	
☐	Ein Malware-Schutz ist installiert und stets aktuell.	
☐	Ein Patch-/Update-Management hält Betriebssysteme und Software aktuell.	
☐	Systeme sind sicher konfiguriert; ungenutzte Dienste und Standardkonten sind deaktiviert.	
☐	Der Fernzugriff erfolgt über ein VPN oder einen gleichwertig gesicherten Kanal.	
☐	Sicherheitsereignisse werden überwacht (Protokollierung / Angriffserkennung je nach Größe).	

§4**Verschlüsselung**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Alle Daten in der Übertragung werden per TLS (HTTPS) verschlüsselt – siehe Abschnitt Website-Sicherheit.	
☐	Personenbezogene Daten im Ruhezustand sind verschlüsselt (Datenbanken, Dateispeicher).	
☐	Auf allen Laptops und Mobilgeräten ist eine Festplattenverschlüsselung aktiviert.	

§4 Verschlüsselung		
ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Backups sind verschlüsselt.	
☐	Sensible Daten per E-Mail werden verschlüsselt (S/MIME, PGP) oder über ein sicheres Portal geteilt.	
§5 Pseudonymisierung & Anonymisierung		
ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Personenbezogene Daten werden pseudonymisiert, wo möglich (Kennungen getrennt vom Inhalt gespeichert).	
☐	Analysedaten werden anonymisiert (z. B. IP-Maskierung) – siehe cookiefreie Analyse-Konfiguration.	
☐	Test- und Entwicklungsumgebungen nutzen anonymisierte oder synthetische Daten, niemals echte personenbezogene Daten.	
§6 Weitergabekontrolle		
ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Daten werden nur über dokumentierte, sichere Kanäle übermittelt.	
☐	Mit jedem Auftragsverarbeiter besteht ein Auftragsverarbeitungsvertrag (Art. 28) – siehe §11.	
☐	Dateien werden verschlüsselt übertragen; sensible Daten werden nie unverschlüsselt per E-Mail versandt.	
☐	Übermittlungen personenbezogener Daten an Dritte werden protokolliert.	
☐	Drittlandübermittlungen stützen sich auf eine dokumentierte Garantie (z. B. SVK) – konsistent mit dem VVT.	
§7 Eingabekontrolle & Datensparsamkeit		
ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Protokolle erfassen, wer wann personenbezogene Daten eingeben, geändert oder gelöscht hat.	
☐	Protokolle sind manipulationsgeschützt und werden angemessen aufbewahrt.	
☐	Es werden nur die für den jeweiligen Zweck erforderlichen Daten erhoben (Datensparsamkeit).	
☐	Aufbewahrungs- und Löschfristen sind definiert und werden angewendet.	

§8**Verfügbarkeit & Belastbarkeit**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Backups laufen regelmäßig und automatisch (nach dem 3-2-1-Prinzip).	
☐	Backups werden durch regelmäßige Wiederherstellung getestet.	
☐	Ein Notfall-/Business-Continuity-Plan ist dokumentiert.	
☐	Strom- und Hardware-Redundanz besteht, wo angemessen (USV, redundanter Speicher).	
☐	Wiederherstellungsziele (RPO/RTO) sind definiert.	

§9**Trennungskontrolle**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Daten werden nach Zweck getrennt (logisch oder physisch).	
☐	Produktions-, Test- und Entwicklungsumgebungen sind getrennt.	
☐	In geteilten/mandantenfähigen Systemen sind Kundendaten logisch getrennt.	

§10**Auftragskontrolle (Art. 28)**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Mit jedem Auftragsverarbeiter besteht ein Auftragsverarbeitungsvertrag (AVV).	
☐	Auftragsverarbeiter werden nach hinreichenden Garantien angemessener Sicherheit ausgewählt (Art. 28 Abs. 1).	
☐	Eine aktuelle Liste der Auftragsverarbeiter wird geführt – konsistent mit dem VVT.	
☐	Die Sicherheit der Auftragsverarbeiter wird regelmäßig überprüft.	
☐	Unterauftragsverarbeiter werden nur mit dokumentierter Genehmigung eingesetzt.	

§11**Datenschutzmanagement & Reaktion auf Vorfälle**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Ein DSB oder Datenschutz-Ansprechpartner ist benannt und erreichbar.	
☐	Ein Verzeichnis von Verarbeitungstätigkeiten (Art. 30) wird geführt – siehe VVT-Vorlage.	
☐	Mitarbeitende sind im Datenschutz geschult und auf Vertraulichkeit verpflichtet.	

§11**Datenschutzmanagement & Reaktion auf Vorfälle**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Ein Prozess zur Meldung von Datenpannen erfüllt die 72-Stunden-Frist (Art. 33).	
☐	Ein Prozess bearbeitet Betroffenenanfragen innerhalb eines Monats (Art. 15-22).	
☐	Diese TOM werden mindestens jährlich überprüft (Art. 32 Abs. 1 lit. d).	

§12**Datenschutz durch Technikgestaltung & Voreinstellungen (Art. 25)**

ERL.	MAßNAHME	STATUS / NOTIZEN
☐	Der Datenschutz wird bei der Gestaltung neuer Prozesse oder Systeme berücksichtigt.	
☐	Voreinstellungen sind datenschutzfreundlich (minimale Daten, kürzeste Aufbewahrung).	
☐	Bei hohem Risiko wird eine DSFA durchgeführt (Art. 35) – siehe DSFA-Vorlage.	

Diese Checkliste dient nur als Orientierung und stellt keine Rechtsberatung dar. Basiert auf Verordnung (EU) 2016/679 (DSGVO). Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E). Bereitgestellt von ETHYX – ethyx.eu.
DSGVO-Höchststrafe: 20 Mio. € / 4 % Umsatz. Version 1.1 · Juli 2026.