

# Technische und organisatorische Maßnahmen (TOM)

---

**Stand:** 13. Jul 2026 · gemäß Art. 32 DSGVO

EZTO betreibt ein an ISO/IEC 27001 ausgerichtetes Informationssicherheits-Managementsystem (ISMS) und befindet sich derzeit im Zertifizierungsprozess nach ISO/IEC 27001. Entsprechende Nachweise (TOM-Dokumentation, Prüfberichte unabhängiger Dritter) werden auf Anfrage bereitgestellt, das Zertifikat nach Erteilung. Die Maßnahmen unterliegen dem Stand der Technik und der Weiterentwicklung; das Sicherheitsniveau wird dabei nicht unterschritten.

## 1. Vertraulichkeit

- Zutrittskontrolle: Hosting in zertifizierten EU-Rechenzentren (Scaleway, Region Paris); physische Sicherung durch den Infrastruktur-Anbieter.
- Zugangskontrolle: Authentifizierung mit Multi-Faktor-Authentisierung (MFA) für administrative Zugänge; rollenbasierte Rechtevergabe (RBAC) nach dem Least-Privilege-Prinzip.
- Zugriffskontrolle: Need-to-know, rollenbasierte Zugriffe, Zugriffsprotokollierung; Beschränkung administrativer Zugriffe.
- Trennungskontrolle: logische Mandantentrennung; im § 203-Modus ein vom Normalbetrieb getrennter Tenant mit eigener, isolierter Wissensbasis.
- Pseudonymisierung/Datenminimierung, soweit für den Zweck möglich.

## 2. Integrität

- Transportverschlüsselung mit TLS 1.2 oder höher für Daten in Übertragung.
- Verschlüsselung ruhender Daten und Artefakte mit AES-256 (mindestens).
- Eingabe- und Weitergabekontrolle; Protokollierung relevanter Aktionen.

## 3. Verfügbarkeit und Belastbarkeit

- Datensicherung (Backups) mit definierten Lösch-/Überschreibzyklen (bis 90 Tage); Inhaltsdaten sind im Zero-Data-Retention-Betrieb ausgenommen.
- Monitoring, Incident-Response-Prozess sowie Business-Continuity-/Notfallkonzept; regelmäßige Überprüfung der Wirksamkeit.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- ISMS nach ISO/IEC 27001 (in Zertifizierung); regelmäßige Penetrationstests; Schwachstellenmanagement; Secure Software Development Lifecycle (Secure SDLC).
- Auftrags- und Subprozessor-Kontrolle: sorgfältige Auswahl, vertragliche Bindung mindestens gleichwertig (Art. 28 Abs. 4 DSGVO), Flow-down der Pflichten.

## 5. Verschlüsselung und Schlüsselverwaltung

- Verschlüsselung in Übertragung (TLS 1.2 oder höher) und ruhender Daten/Artefakte (AES-256 (mindestens)).
- Anbieterverwaltete Schlüssel; ein „Bring Your Own Key“ (BYOK) wird derzeit nicht angeboten.

## 6. KI-Verarbeitung

- Keine Nutzung von Kundeninhalten zum Training; EU-basiertes Routing über Cortecs; Zero Data Retention, soweit verfügbar.

- Im § 203-Modus ausschließlich EU-/EU-kontrollierte Modelle, Websuche deaktiviert (vgl. Verschwiegenheitsvereinbarung).

# Technical and Organizational Measures (TOM)

---

*English convenience translation. Only the German version is legally binding.*

**Last updated:** 13 Jul 2026

pursuant to Art. 32 GDPR

EZTO operates an ISO/IEC 27001-aligned information security management system (ISMS) and is currently undergoing ISO/IEC 27001 certification. Corresponding evidence (TOM documentation, independent third-party audit reports) is provided upon request, and the certificate once issued. The measures are state-of-the-art and subject to further development; the level of security shall not be reduced.

## 1. Confidentiality

- Physical access control: hosting in certified EU data centers (Scaleway, Paris region); physical security by the infrastructure provider.
- System access control: authentication with multi-factor authentication (MFA) for administrative access; role-based assignment of rights (RBAC) on a least-privilege basis.
- Data access control: need-to-know, role-based access, access logging; restriction of administrative access.
- Separation control: logical tenant separation; in § 203 mode, a tenant separated from normal operation with its own, isolated knowledge base.
- Pseudonymization/data minimization to the extent possible for the purpose.

## 2. Integrity

- Transport encryption with TLS 1.2 or higher for data in transit.
- Encryption of data and artifacts at rest with AES-256 (at minimum).
- Input and transfer control; logging of relevant actions.

## 3. Availability and resilience

- Data backup with defined deletion/overwrite cycles (up to 90 days); content data is excluded under zero-data-retention operation.
- Monitoring, incident-response process, and a business continuity/emergency plan; regular review of effectiveness.

## 4. Procedures for regular review, assessment, and evaluation

- ISMS pursuant to ISO/IEC 27001 (undergoing certification); regular penetration testing; vulnerability management; secure software development lifecycle (secure SDLC).
- Order and subprocessor control: careful selection, contractual binding at least equivalently (Art. 28 (4) GDPR), flow-down of obligations.

## 5. Encryption and key management

- Encryption in transit (TLS 1.2 or higher) and of data/artifacts at rest (AES-256 (at minimum)).
- Provider-managed keys; "Bring Your Own Key" (BYOK) is not currently offered.

## 6. AI processing

- No use of customer content for training; EU-based routing via Cortecs; zero data retention where available.
- In § 203 mode, exclusively EU/EU-controlled models, web search deactivated (see the confidentiality agreement).