Technische und organisatorische Maßnahmen (TOM)

Technical and Organizational Measures (TOM)

Stand: 06. Jun 2026

DEUTSCH	ENGLISH (US)
gemäß Art. 32 DSGVO	pursuant to Art. 32 GDPR
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.	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. Vertraulichkeit	**1. Confidentiality**
• Zutrittskontrolle: Hosting in zertifizierten EU-Rechenzentren (Scaleway, Region Paris); physische Sicherung durch den Infrastruktur-Anbieter.	• Physical access control: hosting in certified EU data centers (Scaleway, Paris region); physical security by the infrastructure provider.
• Zugangskontrolle: Authentifizierung mit Multi-Faktor-Authentisierung (MFA) für administrative Zugänge; rollenbasierte Rechtevergabe (RBAC) nach dem Least-Privilege-Prinzip.	• System access control: authentication with multi-factor authentication (MFA) for administrative access; role-based assignment of rights (RBAC) on a least-privilege basis.
• Zugriffskontrolle: Need-to-know, rollenbasierte Zugriffe, Zugriffsprotokollierung; Beschränkung administrativer Zugriffe.	• Data access control: need-to-know, role-based access, access logging; restriction of administrative access.
• Trennungskontrolle: logische Mandantentrennung; im § 203-Modus ein vom Normalbetrieb getrennter Tenant mit eigener, isolierter Wissensbasis.	• Separation control: logical tenant separation; in § 203 mode, a tenant separated from normal operation with its own, isolated knowledge base.
• Pseudonymisierung/Datenminimierung, soweit für den Zweck möglich.	• Pseudonymization/data minimization to the extent possible for the purpose.
2. Integrität	**2. Integrity**
• Transportverschlüsselung mit TLS 1.3 für Daten in Übertragung.	• Transport encryption with TLS 1.3 for data in transit.
• Verschlüsselung ruhender Daten und Artefakte mit AES-256-GCM.	• Encryption of data and artifacts at rest with AES-256-GCM.
• Eingabe- und Weitergabekontrolle; Protokollierung relevanter Aktionen.	• Input and transfer control; logging of relevant actions.
3. Verfügbarkeit und Belastbarkeit	**3. Availability and resilience**
• Datensicherung (Backups) mit definierten Lösch-/Überschreibzyklen (bis 90 Tage); Inhaltsdaten sind im Zero-Data-Retention-Betrieb ausgenommen.	• Data backup with defined deletion/overwrite cycles (up to 90 days); content data is excluded under zero-data-retention operation.
• Monitoring, Incident-Response-Prozess sowie Business-Continuity-/Notfallkonzept; regelmäßige Überprüfung der Wirksamkeit.	• Monitoring, incident-response process, and a business continuity/emergency plan; regular review of effectiveness.
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	**4. Procedures for regular review, assessment, and evaluation**
• ISMS nach ISO/IEC 27001 (in Zertifizierung); regelmäßige Penetrationstests; Schwachstellenmanagement; Secure Software Development Lifecycle (Secure SDLC).	• ISMS pursuant to ISO/IEC 27001 (undergoing certification); regular penetration testing; vulnerability management; secure software development lifecycle (secure SDLC).

DEUTSCH	ENGLISH (US)
• Auftrags- und Subprozessor-Kontrolle: sorgfältige Auswahl, vertragliche Bindung mindestens gleichwertig (Art. 28 Abs. 4 DSGVO), Flow-down der Pflichten.	• Order and subprocessor control: careful selection, contractual binding at least equivalently (Art. 28 (4) GDPR), flow-down of obligations.
5. Verschlüsselung und Schlüsselverwaltung	**5. Encryption and key management**
• Verschlüsselung in Übertragung (TLS 1.3) und ruhender Daten/Artefakte (AES-256-GCM).	• Encryption in transit (TLS 1.3) and of data/artifacts at rest (AES-256-GCM).
• Anbieterverwaltete Schlüssel; ein „Bring Your Own Key" (BYOK) wird derzeit nicht angeboten.	• Provider-managed keys; "Bring Your Own Key" (BYOK) is not currently offered.
6. KI-Verarbeitung	**6. AI processing**
• Keine Nutzung von Kundeninhalten zum Training; EU-basiertes Routing über Cortecs; Zero Data Retention, soweit verfügbar.	• No use of customer content for training; EU-based routing via Cortecs; zero data retention where available.
• Im § 203-Modus ausschließlich EU-/EU-kontrollierte Modelle, Websuche deaktiviert (vgl. Verschwiegenheitsvereinbarung).	• In § 203 mode, exclusively EU/EU-controlled models, web search deactivated (see the confidentiality agreement).