



Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Stand: 02.10.2026 · EFINITI Services GmbH

Diese Übersicht beschreibt die Maßnahmen, mit denen wir die Sicherheit der Verarbeitung gewährleisten. Sie ist Anlage zum Auftragsverarbeitungsvertrag. Details, deren Veröffentlichung die Sicherheit gefährden würde, stellen wir Kunden im Rahmen von Prüfungen zur Verfügung.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- ◆ Unsere Plattform betreiben wir in nach ISO/IEC 27001 zertifizierten Rechenzentren in Deutschland. Eingesetzte Subprozessoren, einschließlich der Anbieter von KI-Modellen, führt die Subprozessor-Liste auf.

1.2 Zugangs- und Zugriffskontrolle

- ◆ Rollen- und Rechtekonzept je Organisation; Sichtbarkeit nach Rechte-Tabelle; private Bereiche sind nur für ihre Eigentümer zugänglich.
- ◆ Mandantengrenzen werden serverseitig erzwungen; unzulässige Zugriffe werden abgewiesen.
- ◆ Auf Wunsch dedizierte Instanz je Kunde.
- ◆ Plattform-Administration ausschließlich durch berechtigte Personen, nicht durch automatisierte Agenten.
- ◆ Jeder KI-Agent verfügt über eine eigene kryptographische Identität, die gesperrt werden kann.
- ◆ Zugangsdaten werden in einem gesicherten Tresor verwahrt und nicht im Klartext in Gesprächen oder Protokollen geführt.
- ◆ Der Zugang erfolgt über eine zentrale Identitäts- und Zugriffsverwaltung. Administrative Zugänge sind auf einen engen, berechtigten Personenkreis beschränkt.

1.3 Trennungskontrolle

- ◆ Logische Trennung der Daten je Mandant; optional physisch getrennte Instanz.

1.4 Pseudonymisierung

- ◆ Für die Verarbeitung durch KI-Modelle steht eine Pseudonymisierung personenbezogener Daten zur Verfügung. Auf unserer Plattform ist sie aktiv.

2. Integrität

2.1 Weitergabekontrolle

- ◆ Externe Zugänge ausschließlich verschlüsselt über TLS.
- ◆ Ausgehender Datenverkehr der KI-Agenten läuft über einen kontrollierten Proxy.
- ◆ Interne Dienste kommunizieren in einem abgeschotteten, nicht öffentlich erreichbaren Netz.

2.2 Eingabekontrolle

- ◆ Sicherheitsrelevante Ereignisse werden in einer Prüfspur protokolliert, die nur fortgeschrieben und nicht verändert werden kann.
- ◆ Aktionen von KI-Agenten sind protokolliert und nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit

- ◆ Daten werden regelmäßig gesichert, die Sicherungen werden in einem Rechenzentrum in Frankfurt am Main aufbewahrt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- ◆ Codeänderungen nur nach Prüfung im Vier-Augen-Prinzip und automatisierten Tests; Freigabe vor Inbetriebnahme.
- ◆ Systeme und Container-Images werden regelmäßig aktualisiert und beim Bau auf bekannte Schwachstellen geprüft.
- ◆ Interne Sicherheitsprüfung alle 14 Tage anhand eines Kontrollkatalogs.
- ◆ Automatische Meldung ausgewählter Sicherheitsereignisse an den Betrieb; Ausbau läuft.

5. Auftragskontrolle

- ◆ Einsatz von Subprozessoren nur auf Grundlage von Verträgen nach Art. 28 DSGVO; Auswahl unter Berücksichtigung ihrer Zertifizierungen.
- ◆ Verpflichtung aller Beschäftigten auf Vertraulichkeit.

6. Datenschutz-Management und Vorfälle

- ◆ Verletzungen des Schutzes personenbezogener Daten melden wir dem Verantwortlichen unverzüglich nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO.
- ◆ Protokolle bewahren wir nur so lange auf, wie es für Sicherheit und Nachvollziehbarkeit erforderlich ist, und löschen sie anschließend, soweit keine gesetzliche Aufbewahrungspflicht besteht.