Anlage II: Technische und organisatorische Massnahmen (TOMs)

Zur Gewährleistung der Sicherheit der Verarbeitung gemäss Art. 32 DSGVO sowie Art. 7 und 8 des Schweizer Datenschutzgesetzes (revDSG) hat apexAI nachfolgende Massnahmen implementiert. Diese orientieren sich am aktuellen Stand der Technik, den Implementierungskosten sowie der Art, dem Umfang und den Zwecken der Verarbeitung.

1. Vertraulichkeit

- **Zugangskontrolle:**
  - Zugriff auf alle von apexAI genutzten Systeme erfolgt ausschliesslich über passwortgeschützte Benutzerkonten.
  - Die Server-Infrastruktur wird vollständig bei zertifizierten Cloud-Anbietern (z. B. AWS, ISO 27001 zertifiziert) gehostet. Der physische Zutritt dort obliegt dem Provider.
  - Büroräume sind durch Schliesssysteme gesichert.
  - Multi-Faktor-Authentifizierung (MFA) ist für alle relevanten Anwendungen und Dienste aktiviert.
  - Sensible Unterlagen werden nicht offen liegen gelassen; Computer werden beim Verlassen des Arbeitsplatzes gesperrt.
  - Zugangsdaten werden in einem Passwortmanager sicher verwaltet.
- **Transportkontrolle:**
  - Alle Datenübertragungen zwischen Systemen und Subprozessoren sind durch TLS/SSL-Verschlüsselung geschützt.
  - Es werden keine sensiblen Daten unverschlüsselt per E-Mail oder über unsichere Kanäle übertragen.
- **Geheimhaltungsverpflichtung:**
  - Alle Mitarbeitenden und etwaige externe Dienstleister sind zur Geheimhaltung verpflichtet und geschult, um den Datenschutz einzuhalten.
  - Daten verschiedener Kunden (Mandanten) werden systemseitig (logisch) getrennt verarbeitet, sodass eine Vermischung ausgeschlossen ist.

2. Integrität

- **Eingabekontrolle:**
  - Änderungen an personenbezogenen Daten werden protokolliert, soweit die eingesetzten Subprozessoren dies unterstützen.
  - Alle Datenverarbeitungen erfolgen gemäss dokumentierten Prozessen und Vorgaben.
- **Weitergabekontrolle:**
  - apexAI gibt personenbezogene Daten nur an autorisierte Subprozessoren weiter, mit denen ein Auftragsverarbeitungsvertrag (ADV) besteht.
  - Jeder Subprozessor wird vor der Zusammenarbeit geprüft, um sicherzustellen, dass er die Datenschutzanforderungen erfüllt.

3. Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle:**
  - Die Datenverfügbarkeit wird durch die von Subprozessoren bereitgestellten Cloud-Dienste sichergestellt (z. B. AWS, Make.com).
  - Backups und Wiederherstellungspläne werden gemäss den Bestimmungen der Subprozessoren durchgeführt.
- **Notfallmanagement:**
  - apexAI hat einen Notfallplan, um bei Ausfällen von Subprozessoren schnell alternative Lösungen zu finden und den Datenzugriff sicherzustellen.

4. Datenminimierung

- **Datensparsamkeit:**
  - apexAI erhebt und verarbeitet ausschliesslich die für den jeweiligen Zweck notwendigen Daten.
  - Personenbezogene Daten werden pseudonymisiert oder anonymisiert, wo dies möglich und sinnvoll ist.
- **Speicherbegrenzung:**
  - Nicht mehr benötigte Daten werden durch automatisierte Prozesse gelöscht, sofern keine gesetzlichen Aufbewahrungsfristen bestehen.

5. Überwachung und Prüfung

- **Protokollierung:**
  - apexAI überprüft regelmässig die Sicherheitsmassnahmen der genutzten Dienste und dokumentiert diese.
  - Sicherheitsvorfälle werden umgehend gemeldet und bearbeitet.

Regelmässige Überprüfung

Die oben genannten Massnahmen werden Periodisch überprüft und an aktuelle technische Standards sowie gesetzliche Anforderungen angepasst.

Hinweis

Diese TOMs gelten für alle Datenverarbeitungsvorgänge durch apexAI sowie deren Subprozessoren, soweit anwendbar.

Stand: Dezember 2025