EuGPT

ANLAGE NACH ART. 32 DSGVO

Technische und organisatorische Maßnahmen

Fassung 1.0 · gültig seit 17.07.2026

Die folgenden Maßnahmen bilden die Standardanlage des EuGPT-AVV. Kundenspezifische oder infrastrukturelle Ergänzungen können gleichwertige oder höhere Schutzmaßnahmen vorsehen. Sicherheitskritische Betriebsdetails werden im Rahmen berechtigter Prüfungen vertraulich bereitgestellt.

KONTROLLBEREICH 01

Zutrittskontrolle

Unbefugten physischen Zutritt zu Verarbeitungssystemen verhindern.

- Betrieb der Kerninfrastruktur in deutschen Rechenzentrumsumgebungen mit geregeltem Zutritt
- Zutrittsberechtigungen nach Aufgabenbezug und Need-to-know-Prinzip
- Dokumentierte Vergabe und Entziehung physischer Berechtigungen

KONTROLLBEREICH 02

Zugangs- und Authentisierungskontrolle

Unbefugte Nutzung von Systemen und Konten verhindern.

- Personenbezogene Benutzerkonten und rollenbasierte administrative Berechtigungen
- Sichere Passwort-Hashes und geschützte, zeitlich begrenzte Sitzungen
- Begrenzung administrativer Zugänge auf autorisierte Beschäftigte
- Protokollierung sicherheitsrelevanter administrativer Vorgänge

KONTROLLBEREICH 03

Zugriffs- und Mandantentrennung

Sicherstellen, dass Daten nur im Rahmen der jeweiligen Berechtigung verarbeitet werden.

- Anwendungsseitige Prüfung von Eigentümerschaft und Berechtigungen
- Trennung von Benutzer-, Chat-, Projekt- und API-Daten anhand der jeweiligen Kontozuordnung
- Gesonderte Administratorrolle mit protokollierten Administrationsvorgängen
- Server- und Modellzugriffe nach Freigabe und Zugriffstyp

KONTROLLBEREICH 04

Übertragungs- und Weitergabekontrolle

Daten bei Übertragung schützen und Empfänger nachvollziehbar begrenzen.

- Verschlüsselte HTTPS-Verbindungen im Produktivbetrieb
- Verschlüsselte Speicherung externer Provider-Zugangsdaten in der Anwendung
- Dokumentierte Auswahl und Freigabe externer KI-Provider
- Keine Nutzung von Kundeneingaben zum Training eigener Self-Hosted-Modelle

KONTROLLBEREICH 05

Eingabe- und Protokollkontrolle

Wesentliche Änderungen und administrative Zugriffe nachvollziehbar machen.

- Audit-Protokoll für administrative Tätigkeiten
- Nutzungs- und Accounting-Datensätze mit Benutzer-, Modell- und Zeitbezug
- Begrenzte Aufbewahrung technischer Protokolle nach festgelegtem Löschkonzept

KONTROLLBEREICH 06

Verfügbarkeit und Wiederherstellung

Verfügbarkeit und zeitnahe Wiederherstellbarkeit personenbezogener Daten unterstützen.

- Betriebsmonitoring für Plattform- und Inferenzkomponenten
- Regelmäßige Datensicherungen nach internem Sicherungskonzept
- Dokumentierte Behandlung technischer Störungen und Sicherheitsvorfälle
- Wiederherstellungsverfahren für relevante Plattformdaten

KONTROLLBEREICH 07

Datenschutzfreundliche Organisation

Datenschutzanforderungen über den gesamten Verarbeitungszyklus berücksichtigen.

- Vertraulichkeitsverpflichtung für berechtigte Beschäftigte
- Weisungsgebundene Verarbeitung und definierte Datenschutzkontakte
- Verfahren für Auskunft, Berichtigung, Export und Löschung
- Prüfung von Unterauftragsverarbeitern vor deren Einsatz
- Regelmäßige Überprüfung der Angemessenheit der Maßnahmen

Überprüfung und Änderung

intercolo überprüft die Angemessenheit der Maßnahmen regelmäßig sowie anlassbezogen. Technische oder organisatorische Änderungen sind zulässig, sofern das vereinbarte Schutzniveau nicht unterschritten wird.