Anlage 1: Technische und organisatorische Maßnahmen

Ente AVV - Version 1.0 - 22. Oktober 2026

Diese Anlage beschreibt Schutzmechanismen und deren Umfang für den gehosteten Ente-Dienst. Sie enthält keine Zusage einer Zertifizierung, Ende-zu-Ende-Verschlüsselung, vollständigen Dateisicherung oder einer bestimmten Verfügbarkeits-, Reaktions- oder Wiederherstellungsfrist. Die Pflicht zu angemessenen Maßnahmen nach Artikel 32 DSGVO bleibt unberührt. Zusätzliche Anforderungen werden vor Beginn des betroffenen Auftrags geklärt.

1. Zugang und Berechtigungen

Ente verwendet authentifizierte Konten sowie serverseitige Prüfungen von Nutzeridentität, Bereichsmitgliedschaften und Berechtigungen. Inhalte werden persönlichen oder gemeinsamen Bereichen zugeordnet. Zugriff über Anwendung, API, CLI und Agenten unterliegt den dafür vorgesehenen Identitäten und Berechtigungen. Freigaben und gemeinsame Bereiche müssen durch berechtigte Nutzer eingerichtet und geprüft werden; eine Firmenzugehörigkeit allein ersetzt diese Prüfung nicht.

Administrative und betriebliche Zugriffe werden auf berechtigte Personen und erforderliche Zwecke begrenzt. Administrativer Zugriff ist technisch möglich und wird nicht als ausgeschlossen dargestellt. Der Kunde verwaltet seine Nutzer und Freigaben; der Anbieter verantwortet die von ihm betriebenen Schutzmechanismen. Entfallende Berechtigungen und Integrationszugänge werden widerrufen. Allgemeine Mehrfaktorauthentifizierung für sämtliche Ente-Endnutzer wird durch diese Anlage nicht zugesichert.

2. Übertragung, Speicherung und Geheimnisse

Die bereitgestellten Web- und Backendzugänge verwenden HTTPS. Der zentrale Convex-Produktionsstandort ist Irland. Die Auslieferung über Netlify einschließlich des vorgesehenen Proxys für private Dateiabfragen ist Teil der Verarbeitung und nicht auf öffentliche statische Dateien beschränkt. Relevante zusätzliche Empfänger stehen in Anlage 2.

Integrationszugänge werden serverseitig verwaltet. Die Anwendung enthält zusätzliche Verschlüsselungsmechanismen für unterstützte Provider-Zugangsdaten und berechtigungsgebundene Abrufmechanismen für private Dateien. Hieraus folgt keine Aussage, dass jeder historische Datensatz bereits vollständig bereinigt oder jede Datenkategorie zusätzlich auf Anwendungsebene verschlüsselt ist. Die Verschlüsselungs- und Zugriffsmaßnahmen der Infrastruktur werden durch deren vertragliche und technische Unterlagen ergänzt. Eine Ende-zu-Ende-Verschlüsselung gegenüber Ente oder den für die Funktion benötigten Verarbeitern besteht nicht.

Zugangsdaten werden nicht in öffentliche Dokumente oder Kundenkorrespondenz aufgenommen. Supportanfragen sollen keine Passwörter oder Zugriffstoken enthalten. Administrative Geheimnisse und der Zugang zu ihrer Verwaltung gehören nicht zur gewöhnlichen Kundenschnittstelle.

3. Datenminimierung und Integrationen

E-Mail-, Kalender- und andere Verbindungen werden nur im eingerichteten und berechtigten Funktionsumfang genutzt. Aufträge und Agentenhandlungen müssen durch die jeweilige Identität und Freigabe gedeckt sein. Für KI-Funktionen werden beauftragte Inhalte und ausgewählter Kontext verarbeitet. Ein vollständiger Ausschluss jeglicher anbieterseitiger Speicherung oder internationaler Verarbeitung wird nicht zugesichert.

Das Abschalten einer Verbindung und die Löschung bereits importierter Kundeninhalte sind unterschiedliche Vorgänge. Aufbewahrung und Löschung richten sich nach Datenkategorie, Kundenweisung und gesetzlichen Pflichten. Die eingeschränkten Einzel- und Kontofunktionen werden nicht als vollständiger automatischer Firmenexport oder als umfassende automatische Kontolöschung dargestellt. Erforderliche umfassendere Auskunft, Rückgabe und Löschung werden über support@ente.fast koordiniert und nach Berechtigungs- und Bestandsprüfung durchgeführt.

4. Betrieb, Änderungen und Überwachung

Produktänderungen durchlaufen eine getrennte Entwicklungsumgebung, automatisierte Prüfungen und einen dokumentierten Überprüfungs- und Bereitstellungsablauf. Fiktive Testbestände werden für gewöhnliche Entwicklungs- und Abnahmetests verwendet. Kundeninhalte werden nicht ohne hierfür bestehende Berechtigung als Testbestände übernommen.

Technische Ausführungs-, Fehler- und Zustandsinformationen unterstützen die Erkennung und Eingrenzung von Störungen. Ihr Zugriff wird betrieblich beschränkt. Eine lückenlose automatische Überwachung jeder Kundenfunktion, ein ununterbrochen besetzter Bereitschaftsdienst oder eine bestimmte Behebungszeit wird nicht zugesichert. Sicherheitsmeldungen werden nach Dringlichkeit geprüft, dokumentiert und bei personenbezogenen Datenschutzverletzungen gemäß AVV weitergegeben.

5. Sicherung und Wiederherstellung

Für den Convex-Produktionsbestand ist eine native wöchentliche Datenbanksicherung eingestellt. Dateispeicher ist von dieser Sicherung ausgeschlossen. Die Sicherung deckt daher nicht sämtliche hochgeladenen Dateien oder Audiodateien ab. Eigene Ursprungsdateien sollten bis zur vereinbarten Klärung ihrer Aufbewahrung verfügbar bleiben.

Aus der eingestellten Sicherung folgt keine Zusage eines bereits durchgeführten vollständigen Wiederherstellungstests, einer unterbrechungsfreien Verfügbarkeit oder eines bestimmten maximalen Datenverlusts. Wiederherstellungen und weitergehende Schutzmaßnahmen werden anhand des tatsächlichen Vorfalls und des vereinbarten Umfangs abgestimmt. Die gesetzlichen und vertraglichen Schutzpflichten werden dadurch nicht eingeschränkt.

6. Organisation und Nachweise

Der Anbieter verantwortet Datenschutzanfragen, Sicherheit und Dienstleisterkoordination. Berechtigte Personen unterliegen Vertraulichkeit; wesentliche administrative Änderungen, Weisungen, Vorfälle und betriebliche Bearbeitungsschritte werden zweckentsprechend dokumentiert. Eine lückenlose Protokollierung jedes administrativen Lesezugriffs wird damit nicht zugesichert. support@ente.fast ist der Kontakt für Support, Sicherheitsmeldungen und Datenanfragen; sales@ente.fast für Vertragsfragen.

Dienstleister werden nach Aufgabe, Datenkategorien, Verarbeitungsländern, vertraglicher Einbindung und gegebenenfalls Übermittlungsschutz erfasst. Neue oder ersetzte weitere Auftragsverarbeiter unterliegen dem Verfahren der AVV. Ergänzende sicherheitsrelevante Nachweise können dem Kunden unter angemessenem Vertraulichkeitsschutz bereitgestellt werden. Die Maßnahmen werden bei wesentlichen Änderungen und im Rahmen der laufenden Betriebsprüfung überprüft.