٩

Wareed — Sicherheit & Datenschutz

Technisches und rechtliches Whitepaper für Legal- & IT-Teams.
Klar dokumentiert, EU-fokussiert, DSGVO-konform — ohne Marketing-Sprech.

Stand: Juni 2026

Zielzustand zum Produkt-Launch — als „geplant" markierte Punkte sind noch nicht aktiv. Dieses Whitepaper beschreibt den Zielzustand zum Produkt-Launch. Aktive Komponenten sind als „aktiv" markiert, geplante als „geplant".

VIER PRINZIPIEN

Worauf wir niemals Kompromisse machen.

١

EU-Hosting

Alle produktiven Daten in EU-Rechenzentren. Geplant: Hetzner Falkenstein (Deutschland) für Anwendungs-Daten. Aktuelle Landingpage läuft via Cloudflare Pages (DPF-zertifiziert, SCC).

٢

Kein KI-Training mit deinen Daten

Deine Mails werden nicht zum Training von KI-Modellen genutzt. Anthropic verarbeitet API-Inhalte gemäß Commercial Terms **nicht** für Modell-Training.

٣

Verschlüsselung

TLS 1.3 für die Übertragung. API-Keys/Secrets ausschließlich als Umgebungsvariablen, nie im Code. Dashboard-Zugang über einen Admin-Token mit konstant-zeitigem Vergleich (Schutz vor Timing-Angriffen). Geplant: Festplatten-Verschlüsselung at-rest und Multi-User-Passwörter mit bcrypt.

٤

Du behältst die Kontrolle

Auf Knopfdruck löschbar. Vollständige Datenexporte jederzeit möglich. Kein Lock-in. Kündigung jederzeit zum Monatsende.

DATENVERARBEITUNG

Was wir speichern werden. Und was nicht.

Vollständige Transparenz über die geplante Architektur. Du siehst genau, welche Daten Wareed verarbeiten wird.

DATENTYP	SPEICHERORT	AUFBEWAHRUNG	STATUS
E-Mail-Inhalte Eingang & generierte Antworten	EU-Server (geplant: Hetzner)	90 Tage rollend	GEPLANT
SOPs & Wissensbasis Deine hochgeladenen Dokumente	EU-Server	Bis Löschung durch dich	GEPLANT
Account-Daten Name, E-Mail, Login	EU-Server	Vertragslaufzeit + 30 Tage	GEPLANT
Nutzungsstatistiken Anzahl Mails, Confidence Scores	EU-Server	12 Monate	GEPLANT
~~**Zahlungsdaten**~~ Wir speichern keine Kreditkarten	— bei Stripe (PCI-DSS)	—	NICHT BEI UNS
~~**E-Mail-Anhänge**~~ Werden nicht verarbeitet	—	—	NIE VERARBEITET

Stand: Mai 2026 · Status „geplant" = Architektur-Entscheidung steht, Implementierung folgt vor Produkt-Launch · Änderungen werden mind. 30 Tage vorher angekündigt.

SUB-PROCESSORS

Mit wem wir zusammenarbeiten werden.

Geplante Liste aller Drittanbieter mit Datenzugriff. AVV mit jedem Anbieter wird vor Produkt-Launch abgeschlossen.

Anthropic USA · DPF-zertifiziert — AVV GEPLANT

KI-Verarbeitung der E-Mails (Claude API). API-Inhalte werden laut Anthropic Commercial Terms nicht zum Training verwendet.

Hetzner Online Deutschland · ISO 27001 — AVV GEPLANT

Server-Hosting in Falkenstein. Vorgesehen für Anwendungs-Server zum Produkt-Launch.

Cloudflare USA · DPF-zertifiziert · SCC — AKTIV

CDN, DDoS-Schutz und SSL für die Landingpage (aktiv). Für produktive App-Endpoints geplant mit EU-Cache-Strategie.

Stripe Irland (EU) · PCI-DSS Level 1 — AVV GEPLANT

Zahlungsabwicklung. Wir sehen keine Kartendaten.

COMPLIANCE

Standards die wir einhalten werden.

DSGVO / GDPR

Architektur ist DSGVO-konform ausgelegt. AVV-Vorlage in Vorbereitung.

in Vorbereitung

EU AI Act

Konzeption mit Transparenzpflichten für KI-Systeme.

geplant

ISO 27001

Zertifizierung für 2027 angestrebt. Hosting-Provider ist bereits ISO-zertifiziert.

2027 geplant

HÄUFIGE FRAGEN

Was Legal-Teams typischerweise fragen.

› Werden unsere E-Mails zum KI-Training verwendet?

Nein. Anthropic (unser geplanter KI-Provider) verwendet API-Inhalte gemäß Commercial Terms nicht zum Modell-Training. Wareed selbst trainiert keine Modelle mit deinen Daten. Beides wird im AVV mit dir vertraglich festgehalten.

› Wo werden die Daten gespeichert?

Geplant: deutsche Rechenzentren (Hetzner Falkenstein) für Anwendungs- und Mail-Daten. Die KI-Verarbeitung über Anthropic erfolgt mit Standard-Vertragsklauseln (SCCs); Anthropic ist DPF-zertifiziert. Sobald Anthropic EU-Endpunkte verfügbar macht, prüfen wir die Migration.

› Wer hat Zugriff auf unsere Mail-Inhalte?

Niemand außer dem System selbst. Mitarbeiter von Wareed haben standardmäßig keinen Zugang zu Mail-Inhalten unserer Kunden. Im Support sehen wir nur Metadaten (Anzahl, Kategorien, Confidence Scores). Ausnahme: explizite Freigabe durch dich für ein konkretes Support-Ticket.

› Was passiert wenn Wareed insolvent wird?

Im Insolvenzfall erhalten alle Kunden 60 Tage vor Einstellung Zugriff auf vollständige Daten-Exports. Das wird im AVV festgelegt. Außerdem: Da Wareed deine Mails nur synchronisiert (nicht migriert), bleiben deine Original-Mails immer in deinem Gmail/Outlook — Wareed ist eine Schicht obendrüber, kein Ersatz-System.

› Wie schnell können wir alle Daten löschen lassen?

Sofort. Im Dashboard wird es einen „Alle Daten löschen"-Button geben (mit Sicherheitsabfrage). Innerhalb von 24 Stunden werden alle Inhalte aus aktiven Systemen gelöscht. Backups werden innerhalb von 30 Tagen rotiert und überschrieben. Bestätigungs-Mail mit Lösch-Protokoll wird automatisch versendet.

› Was passiert bei einer Datenpanne?

Innerhalb von 72 Stunden (DSGVO-Pflicht): vollständige Information aller betroffenen Kunden inklusive (1) Art und Umfang der Panne, (2) wahrscheinliche Folgen, (3) ergriffene Gegenmaßnahmen, (4) Kontakt für Rückfragen. Parallel: Information an die zuständige Datenschutzbehörde.

› Kann Wareed in unsere bestehende Sicherheits-Architektur integriert werden?

Geplant für Enterprise: Single Sign-On (SSO) via SAML/OAuth, IP-Whitelisting, Audit-Logs in dein SIEM, und Bring-Your-Own-Encryption-Key (BYOK) für besonders sensible Setups. Sprich uns an für individuelle Anforderungen.

› Ist Wareed für regulierte Branchen geeignet?

Aktuell empfehlen wir Wareed nicht für Branchen mit besonders hohen Compliance-Anforderungen (Banking, Krankenhäuser mit Patientenakten, Versicherungen mit Gesundheitsdaten). ISO 27001 Zertifizierung ist für 2027 geplant. Sprich uns trotzdem gerne an — Einzelfallprüfung möglich.

ROADMAP & ENTERPRISE

Was als Nächstes kommt.

Geplante Sicherheits- und Compliance-Meilensteine bis zum Produkt-Launch und darüber hinaus.

ISO 27001 Zertifizierung

2027 GEPLANT

Zertifizierung für 2027 angestrebt. Der Hosting-Provider (Hetzner) ist bereits ISO-27001-zertifiziert. Bis dahin empfehlen wir Wareed nicht für Branchen mit besonders hohen Compliance-Anforderungen.

Verschlüsselung at-rest GEPLANT

Festplatten-Verschlüsselung at-rest und Multi-User-Passwörter mit bcrypt sind für den Produkt-Launch geplant. In Übertragung gilt bereits heute TLS 1.3.

Enterprise-Integration GEPLANT

Single Sign-On (SSO) via SAML/OAuth, IP-Whitelisting, Audit-Logs in dein SIEM und Bring-Your-Own-Encryption-Key (BYOK) für besonders sensible Setups. Individuelle Anforderungen auf Anfrage.

AVV & Rechtsdokumente

IN VORBEREITUNG

AVV-Vorlage in Vorbereitung; AVV mit jedem Sub-Processor wird vor Produkt-Launch abgeschlossen. DSGVO-konforme Architektur und EU-AI-Act-Transparenzpflichten sind in der Konzeption berücksichtigt.