M A I L N E X A . A I

SSO & Sicherheit

Business-Paket

Dieses Dokument beschreibt die Sicherheitsarchitektur, Authentifizierung, Datenverschlüsselung und Compliance-Massnahmen von MailNexa.ai.

Version: Stand Februar 2026 – mailnexa.ai

1. Sicherheitsübersicht

MailNexa.ai wurde von Grund auf mit dem Fokus auf Datensicherheit und Datenschutz entwickelt. Alle Systeme befinden sich in der EU/Schweiz, und es findet kein Datentransfer in Drittländer statt.

Bereich	Massnahme
Hosting	Hetzner Rechenzentren in Deutschland – ISO 27001 zertifiziert
Datenhaltung	Ausschliesslich EU/CH – kein Drittland-Transfer
Verschlüsselung (Transit)	TLS 1.2 / 1.3 für alle Verbindungen (HTTPS, IMAP, SMTP)
Verschlüsselung (Ruhe)	AES-256 für gespeicherte Daten und Zugangstokens
Authentifizierung	E-Mail/Passwort + OAuth 2.0 für Gmail/Microsoft
Zugriffskontrolle	Rollenbasiertes System (Admin, Manager, Agent, Beobachter)
Verfügbarkeit	Redundante Systeme mit automatischem Failover – Ziel: 99.9% Uptime
Backups	Tägliche automatische Backups – verschlüsselt und georedundant
Compliance	DSGVO-konform, Schweizer DSG-konform
SLA	24h Support-SLA im Business-Paket

Sicherheitsprinzip:
MailNexa.ai folgt dem Prinzip der minimalen Datenhaltung: Es werden nur die Daten gespeichert, die für den Betrieb zwingend notwendig sind. E-Mail-Inhalte werden für die KI-Analyse verarbeitet und gemäss den konfigurierten Aufbewahrungsfristen gespeichert.

2. Authentifizierung & Zugang

2.1 Standard-Authentifizierung

Die Standard-Anmeldung bei MailNexa.ai erfolgt über E-Mail-Adresse und Passwort.

Anforderung	Details
Passwortlänge	Mindestens 10 Zeichen
Passwortkomplexität	Mindestens 1 Grossbuchstabe, 1 Kleinbuchstabe, 1 Zahl, 1 Sonderzeichen
Passwort-Hashing	bcrypt mit Salt – Passwörter werden nie im Klartext gespeichert
Passwort-Reset	Über E-Mail-Verifizierung – Reset-Links sind 1 Stunde gültig
Account-Sperrung	Nach 5 fehlgeschlagenen Login-Versuchen: 15 Minuten Sperre
Session-Timeout	Automatische Abmeldung nach 24 Stunden Inaktivität

2.2 Zwei-Faktor-Authentifizierung (2FA)

Im Business-Paket kann 2FA für alle Team-Mitglieder aktiviert und erzwungen werden.

Unterstützte 2FA-Methoden

- TOTP (Time-based One-Time Password) – kompatibel mit Google Authenticator, Authy, Microsoft Authenticator
- E-Mail-basierter Code – Einmalcode per E-Mail als Fallback

2FA einrichten

① Im Dashboard: Mein Konto → Sicherheit → Zwei-Faktor-Authentifizierung
② Methode wählen (TOTP empfohlen)
③ QR-Code mit Authenticator-App scannen
④ Bestätigungscode eingeben
⑤ Backup-Codes speichern (einmalig generiert – sicher aufbewahren!)

2FA für das gesamte Team erzwingen

① Im Dashboard: Einstellungen → Sicherheit → 2FA-Pflicht aktivieren
② Alle Team-Mitglieder werden beim nächsten Login aufgefordert, 2FA einzurichten
③ Mitglieder ohne 2FA können sich nach der Aktivierung nicht mehr anmelden

Empfehlung:
Wir empfehlen dringend, 2FA für alle Team-Mitglieder zu aktivieren – insbesondere für Administratoren. Dies schützt vor unbefugtem Zugriff selbst bei kompromittierten Passwörtern.

2.3 OAuth 2.0 für Postfachverbindungen

Beim Verbinden von Gmail- und Microsoft-Postfächern wird OAuth 2.0 verwendet. Dabei werden keine Passwörter an MailNexa übermittelt – stattdessen wird ein verschlüsseltes Zugriffstoken gespeichert.

Aspekt	Details
Protokoll	OAuth 2.0 mit Authorization Code Flow
Token-Speicherung	AES-256 verschlüsselt auf EU/CH-Servern
Token-Erneuerung	Automatische Refresh-Token-Erneuerung – kein manuelles Eingreifen nötig
Widerruf	Jederzeit im MailNexa-Dashboard oder beim Provider (Google/Microsoft) möglich
Scopes (Gmail)	gmail.readonly, gmail.send, gmail.compose, gmail.modify
Scopes (Microsoft)	Mail.ReadWrite, Mail.Send, offline_access

Hinweis:
Bei OAuth 2.0 hat MailNexa zu keinem Zeitpunkt Zugriff auf dein Google- oder Microsoft-Passwort. Du kannst die erteilten Berechtigungen jederzeit bei Google (myaccount.google.com/permissions) oder Microsoft (myapps.microsoft.com) widerrufen.

3. Single Sign-On (SSO)

Verfügbarkeit:
SSO ist als vollständige Lösung im Enterprise-Paket enthalten. Im Business-Paket steht eine vereinfachte SSO-Vorbereitung zur Verfügung: OAuth 2.0-Login über Google und Microsoft. Vollständiges SAML 2.0 / OpenID Connect SSO mit eigenem Identity Provider ist dem Enterprise-Paket vorbehalten.

3.1 SSO im Business-Paket (OAuth-basiert)

Im Business-Paket können sich Team-Mitglieder über ihre bestehenden Google- oder Microsoft-Konten anmelden, anstatt separate Zugangsdaten zu erstellen.

Google-Login aktivieren

① Im Dashboard: Einstellungen → Sicherheit → Anmeldemethoden
② „Mit Google anmelden“ aktivieren
③ Optional: Erlaubte E-Mail-Domains einschränken (z.B. nur @meinefirma.ch)
④ Team-Mitglieder können sich nun per Google-Login anmelden

Microsoft-Login aktivieren

① Im Dashboard: Einstellungen → Sicherheit → Anmeldemethoden
② „Mit Microsoft anmelden“ aktivieren
③ Optional: Nur bestimmte Azure AD-Tenants zulassen
④ Team-Mitglieder können sich nun per Microsoft-Login anmelden

Hinweis:
Die OAuth-basierte Anmeldung im Business-Paket nutzt die Standard-OAuth-Flows von Google und Microsoft. Für vollständiges SSO mit SAML 2.0, OpenID Connect, eigenem Identity Provider (z.B. Okta, Azure AD B2C, Keycloak) oder erzwungenem SSO-Login ist ein Upgrade auf das Enterprise-Paket erforderlich.

3.2 SSO im Enterprise-Paket (Übersicht)

Für Unternehmen mit eigener Identity-Management-Infrastruktur bietet das Enterprise-Paket vollständiges SSO:

Funktion	Business	Enterprise
Google OAuth-Login	✓	✓
Microsoft OAuth-Login	✓	✓
SAML 2.0	–	✓
OpenID Connect (OIDC)	–	✓
Eigener Identity Provider (Okta, Keycloak, etc.)	–	✓
Erzwungener SSO-Login (kein Passwort-Fallback)	–	✓
Automatische User-Provisionierung (SCIM)	–	✓
Domain-basierte Zugangssteuerung	Basis	Erweitert
Conditional Access Policies	–	✓

Interesse am Enterprise-Paket?
Kontaktiere uns unter enterprise@mailnexa.ai oder mailnexa.ai/Informationen/Kontakt für ein individuelles Angebot mit vollständigem SSO, dedizierter Instanz und Custom SLA.

4. Datenverschlüsselung

4.1 Verschlüsselung in Transit

Alle Daten, die zwischen deinem Browser/Client und den MailNexa-Servern übertragen werden, sind durchgehend TLS-verschlüsselt.

Verbindung	Verschlüsselung
Browser ↔ MailNexa-Dashboard	TLS 1.2 / 1.3 (HTTPS) – HSTS aktiviert
MailNexa ↔ IMAP-Server	TLS 1.2 / 1.3 (Port 993) oder STARTTLS (Port 143)
MailNexa ↔ SMTP-Server	TLS 1.2 / 1.3 (Port 465) oder STARTTLS (Port 587)
MailNexa ↔ Google API	TLS 1.3 (OAuth 2.0)
MailNexa ↔ Microsoft Graph API	TLS 1.3 (OAuth 2.0)
MailNexa ↔ Telegram API	TLS 1.2 / 1.3 (HTTPS)
MailNexa ↔ WhatsApp Business API	TLS 1.3 (HTTPS)
MailNexa ↔ KI-Modelle (OpenAI, Anthropic, etc.)	TLS 1.3 (HTTPS) – API-Keys verschlüsselt
Webhook-Auslieferung	HTTPS zwingend – HTTP-Endpoints werden abgelehnt

4.2 Verschlüsselung at Rest

Alle gespeicherten Daten werden mit AES-256 verschlüsselt:

Datentyp	Speicherort	Verschlüsselung
OAuth-Tokens (Gmail, Microsoft)	Datenbank	AES-256 (anwendungsseitig verschlüsselt)
IMAP/SMTP-Zugangsdaten	Datenbank	AES-256 (anwendungsseitig verschlüsselt)
API-Keys	Datenbank	bcrypt-Hash (nicht entschlüsselbar)
E-Mail-Inhalte (Cache)	Datenbank	AES-256 auf Volume-Ebene (Hetzner)
Benutzerpasswörter	Datenbank	bcrypt mit Salt (nicht entschlüsselbar)
Backups	Separater Storage	AES-256 – georedundant (DE)
Log-Dateien	Server	Volume-Verschlüsselung

Kein Klartext:
Passwörter und API-Keys werden niemals im Klartext gespeichert. OAuth-Tokens und IMAP-Zugangsdaten werden anwendungsseitig verschlüsselt – selbst bei physischem Zugriff auf die Datenbank sind sie nicht lesbar.

5. Netzwerk & Infrastruktursicherheit

5.1 Hosting-Infrastruktur

Aspekt	Details
Provider	Hetzner Online GmbH – Rechenzentren in Deutschland
Zertifizierung	ISO 27001, SOC 2 (Hetzner-seitig)
Standort	Falkenstein / Nürnberg, Deutschland
Instanztyp (Business)	Cluster-Instanz – dedizierte Ressourcen, getrennt von Starter/Profi
Betriebssystem	Linux (Ubuntu LTS) – gehärtet, nur notwendige Dienste aktiv
Container-Isolation	Docker-basierte Isolation zwischen Mandanten

5.2 Firewall & Netzwerk

- Eingehend: Nur HTTPS (443) und SSH (Key-Only, kein Passwort) geöffnet
- Ausgehend: Nur notwendige Verbindungen zu Mail-Servern, APIs und Notification-Diensten
- Fail2Ban: Automatische IP-Sperrung nach wiederholten fehlgeschlagenen Anmeldeversuchen
- DDoS-Schutz: Cloudflare als Reverse Proxy mit WAF (Web Application Firewall)
- Internes Netzwerk: Keine öffentlichen IPs für Datenbank- und Backend-Server

5.3 Updates & Patching

- Sicherheitsupdates: Innerhalb von 24 Stunden nach Veröffentlichung kritischer Patches
- Betriebssystem-Updates: Wöchentliche automatische Updates (nicht sicherheitskritisch)
- Applikations-Updates: Rolling Deployments ohne Downtime
- Abhängigkeiten: Automatisierte Schwachstellen-Scans (Dependabot-äquivalent)

5.4 Monitoring & Logging

- Uptime-Monitoring: 24/7 mit automatischem Alerting bei Ausfällen
- Performance-Monitoring: CPU, RAM, Disk, Netzwerk – Schwellenwert-basierte Alerts
- Security-Logging: Alle Anmeldeversuche, Rollenänderungen, API-Zugriffe protokolliert
- Audit-Trail: Wer hat wann welche Einstellung geändert? (einsehbar für Administratoren)
- Log-Retention: 90 Tage Standard, verlängerbar auf Anfrage (Enterprise)

6. Datenschutz & Compliance

6.1 DSGVO-Konformität

MailNexa.ai ist vollständig DSGVO-konform. Die Verarbeitung personenbezogener Daten erfolgt ausschliesslich auf Grundlage eines Auftragsverarbeitungsvertrags (DPA) und im Einklang mit der EU-Datenschutzgrundverordnung sowie dem Schweizer Datenschutzgesetz (DSG).

Anforderung	Umsetzung
Rechtsgrundlage	Auftragsverarbeitung gem. Art. 28 DSGVO
DPA / AVV	Standard-DPA im Business-Paket enthalten
Datenminimierung	Nur für den Betrieb notwendige Daten werden gespeichert
Zweckbindung	Daten werden ausschliesslich für die E-Mail-Automatisierung verwendet
Löschung bei Kündigung	Vollständige Löschung innerhalb von 30 Tagen nach Kündigung
Datenexport	Jederzeit über Dashboard oder auf Anfrage (Art. 20 DSGVO)
Auskunftsrecht	Jederzeit über support@mailnexa.ai (Art. 15 DSGVO)
Kein Drittland-Transfer	Alle Daten verbleiben in der EU/CH – kein Transfer in Drittländer

6.2 KI-Verarbeitung & Datenschutz

MailNexa nutzt externe KI-Modelle (OpenAI, Anthropic, Google, DeepSeek) für die E-Mail-Analyse und Antworterstellung. Dabei gelten folgende Sicherheitsmassnahmen:

Aspekt	Details
Datenübertragung	Verschlüsselt per TLS 1.3 an den jeweiligen KI-Anbieter
Datenverwendung	Kein Training der KI-Modelle mit deinen Daten – alle Anbieter sind vertraglich gebunden
API-Nutzung	Nutzung der Business/Enterprise-APIs der Anbieter (kein Consumer-Tier)
Speicherung beim Anbieter	Keine Speicherung der Anfragen/Antworten durch den KI-Anbieter
Rechtsgrundlage	Auftragsverarbeitung – DPA mit jedem KI-Anbieter abgeschlossen
Opt-Out	Du kannst jederzeit ein Modell deaktivieren und ein anderes wählen

Transparenz:
E-Mail-Inhalte werden zur Analyse und Antworterstellung an den gewählten KI-Anbieter übermittelt. Die Auswahl des Anbieters liegt bei dir. Alle Anbieter sind vertraglich verpflichtet, die Daten nicht für eigene Zwecke (z.B. Modell-Training) zu verwenden. Details zu den einzelnen Anbietern findest du in unserer Datenschutzerklärung unter mailnexa.ai/Shopservice/Datenschutz.

6.3 Aufbewahrung & Löschung

Datentyp	Aufbewahrungsfrist	Löschung
E-Mail-Metadaten (Betreff, Absender, Zeitstempel)	Solange Abo aktiv + 30 Tage	Automatisch nach Kündigung
E-Mail-Inhalte (Cache für KI-Analyse)	Max. 30 Tage oder gemäss Einstellung	Automatische Löschung nach Ablauf
KI-Antwortentwürfe	Solange Abo aktiv	Automatisch nach Kündigung
Zugangsdaten (IMAP/OAuth)	Solange Postfach verbunden	Sofort bei Trennung des Postfachs
Benutzerkonten & Profile	Solange Abo aktiv + 30 Tage	Automatisch nach Kündigung
Logs & Audit-Trail	90 Tage	Automatische Rotation
Backups	30 Tage	Automatische Rotation

Datenexport:
Du kannst jederzeit einen vollständigen Export deiner Daten anfordern. Im Dashboard unter Einstellungen → Daten → Datenexport anfordern. Der Export wird als verschlüsseltes ZIP-Archiv bereitgestellt.

7. API-Sicherheit

Die MailNexa REST API im Business-Paket ist durch mehrere Sicherheitsebenen geschützt:

Massnahme	Details
Authentifizierung	Bearer Token (API-Key) in Authorization-Header
Verschlüsselung	Ausschliesslich HTTPS – HTTP-Requests werden abgelehnt
Rate Limiting	100 Requests/Minute (Standard), erhöhbar auf Anfrage
IP-Whitelisting (optional)	API-Zugriff auf bestimmte IP-Adressen beschränken
Scopes / Berechtigungen	Pro API-Key konfigurierbar (Lesen, Schreiben, Webhooks)
Key-Rotation	Empfohlen alle 90 Tage – alter Key bleibt 24h aktiv nach Deaktivierung
Webhook-Signatur	HMAC-SHA256 Signatur in X-Mailnexa-Signature Header
Audit-Logging	Jeder API-Zugriff wird protokolliert (IP, Zeitstempel, Endpoint)

Sicherheitsregeln für API-Keys:
API-Keys niemals im Quellcode speichern – verwende Umgebungsvariablen. Keys niemals über unverschlüsselte Kanäle teilen. Bei Verdacht auf Kompromittierung: Key sofort deaktivieren und neuen erstellen. Nutze IP-Whitelisting wenn möglich. Vergib pro Integration einen eigenen Key mit minimalen Berechtigungen.

8. Incident Response & Notfallverfahren

MailNexa verfügt über dokumentierte Prozesse für den Umgang mit Sicherheitsvorfällen:

Phase	Massnahme	Zeitrahmen
Erkennung	Automatisierte Überwachung + Alerting bei Anomalien	Sofort
Bewertung	Klassifikation nach Schweregrad (Kritisch/Hoch/Mittel/Niedrig)	< 1 Stunde
Eindämmung	Isolierung betroffener Systeme, Zugriffssperre bei Bedarf	< 2 Stunden
Benachrichtigung	Betroffene Kunden werden informiert (bei Datenschutzvorfällen gem. Art. 33/34 DSGVO)	< 72 Stunden
Behebung	Patch/Fix einspielen, Root-Cause-Analyse	Abhängig vom Vorfall
Nachbereitung	Lessons Learned, Dokumentation, Präventionsmassnahmen	< 2 Wochen

Kontakt bei Sicherheitsvorfällen:
Wenn du einen Sicherheitsvorfall vermutest oder eine Schwachstelle melden möchtest: security@mailnexa.ai – Diese Adresse wird priorisiert bearbeitet. Alternativ: Hotline +41 (0)56 300 00 64.

9. Sicherheits-Checkliste für Business-Kunden

Empfohlene Massnahmen nach der Einrichtung deines Business-Accounts:

Massnahme	Priorität	Status
2FA für alle Administratoren aktivieren	Hoch	☐
2FA-Pflicht für das gesamte Team erzwingen	Hoch	☐
Mindestens 2 Administratoren einrichten	Hoch	☐
Rollen nach Minimalprinzip vergeben	Hoch	☐
Postfachzuordnung nach Abteilungen trennen	Mittel	☐
OAuth-Login (Google/Microsoft) aktivieren	Mittel	☐
E-Mail-Domain für Team-Anmeldung einschränken	Mittel	☐
API-Keys mit minimalen Berechtigungen erstellen	Mittel	☐
IP-Whitelisting für API-Zugriff konfigurieren	Optional	☐
Webhook-Secret für Signaturprüfung hinterlegen	Mittel	☐
Automatische Report-Zustellung für Audit einrichten	Niedrig	☐
Datenschutzerklärung und DPA prüfen/unterzeichnen	Hoch	☐
Regelmässige Rollenüberprüfung (quartalsweise) planen	Mittel	☐

Hilfe & Support

Hotline: +41 (0)56 300 00 64 (Mo–Fr, 09:00–17:00)

E-Mail: support@mailnexa.ai (24h SLA im Business-Paket)

Sicherheit: security@mailnexa.ai (priorisiert)

Kontaktformular: mailnexa.ai/Informationen/Kontakt