Kalima



Sicherheit und Datenschutz bei Kalima.

Technische und organisatorische Maßnahmen

Ihre Aufnahmen liegen auf Servern in Deutschland, sind verschlüsselt und werden nie für KI-Training genutzt. Sie entscheiden, wer sie sieht.

Stand
24. November 2026

Gehört zu
Vertrag zur Auftragsverarbeitung, Version 1.3

Herausgeber
ByteHawk GmbH, Düsseldorf

Auf einen Blick

Die Maßnahmen im Einzelnen, zu Anlage 2 des Vertrags zur Auftragsverarbeitung.

Inhalt

1	Schutz in Schichten	3
2	Anmeldung und Zugriff	4
3	Verschlüsselung und Trennung	5
4	Dienstleister, KI und Löschung	6
5	Protokollierung und Mitbestimmung	7
6	Verfügbarkeit und Betrieb	8
7	Prüfung und Grenzen	9
	Kontakt	10

Kurzfassung

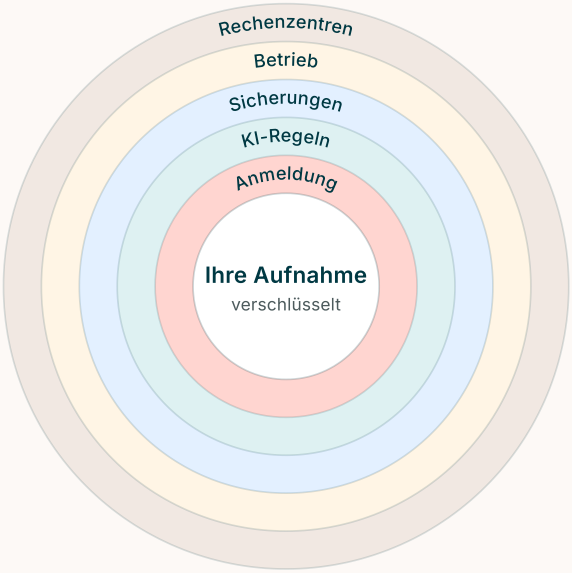
Serverstandort	Deutschland, bei netcup und Hetzner
Rechenzentren	nach ISO 27001 zertifiziert
Verschlüsselung	AES-256-GCM, Audio schon auf Ihrem Gerät
Anmeldung	Zwei-Faktor, Single Sign-on und SCIM 2.0
Spracherkennung und KI	in der EU, kein Training mit Ihren Inhalten
Audit-Log	13 Monate, Export als CSV oder JSON
Löschfristen	30, 90, 180 oder 365 Tage
Sicherung	fortlaufend, jeder Zeitpunkt der letzten sechs Tage
Erreichbarkeit	99,99 % vom 31. Juli bis zum 24. November 2026

Anbieter

Unternehmen	ByteHawk GmbH, Fährstraße 217, 40221 Düsseldorf
Register	Amtsgericht Düsseldorf, HRB 114451
Fragen zur Sicherheit	security@meetkalima.com

1 Schutz in Schichten

Jede Aufnahme liegt hinter sechs Schichten. Die Server stehen in Deutschland.



Verschlüsselung
Audio wird schon auf Ihrem Gerät verschlüsselt. Gespeichert mit AES-256-GCM, mit eigenen Schlüsseln je Aufnahme.

Anmeldung
Zwei-Faktor per App oder Passkey. Nach Fehlversuchen vorübergehend gesperrt.

KI-Regeln
Spracherkennung und KI laufen in der EU. KI-Anbieter speichern nichts. Kein KI-Training mit Ihren Daten.

Sicherungen
Täglich, verschlüsselt, in Deutschland.

Betrieb
Eine Content Security Policy blockiert fremden Code. Laufend überwacht, Schwachstellen behoben.

Rechenzentren
Server in Deutschland, in nach ISO 27001 zertifizierten Rechenzentren.

Standort

Server in Deutschland
Anwendung und Datenbank laufen auf Servern von netcup in Deutschland. Audio und Sicherungen liegen im Objektspeicher von Hetzner in Deutschland.

Zutritt
Die Betreiber der Rechenzentren kontrollieren den physischen Zutritt.

Spracherkennung und KI
Spracherkennung und KI-Verarbeitung laufen in Rechenzentren in der EU.

Rechenzentren

Anbieter	Was dort liegt	Zertifikat nach ISO 27001
netcup	Anwendung und Datenbank	jährlich geprüft vom TÜV NORD
Hetzner	Audio und Sicherungen	zertifiziert von SOCOTEC

Die Zertifikate gelten für die Rechenzentren unserer Hosting-Anbieter.

2 Anmeldung und Zugriff

Wer sich anmelden kann und wer welche Aufnahme öffnen darf.

Anmeldung

Passwörter

Passwörter werden nur als Hash gespeichert (Argon2id). Nach fünf Fehlversuchen ist die Anmeldung 15 Minuten gesperrt.

Zwei-Faktor-Anmeldung

Mit Authentifizierungs-App oder Passkey. Für Inhaber, Admins und alle mit einer Rolle in der Console ist sie Pflicht. Ihre Firma kann sie für alle Mitglieder verlangen.

Sitzungen

Die Console meldet nach 30 Minuten ohne Aktivität ab, spätestens nach 12 Stunden. Kritische Aktionen verlangen den zweiten Faktor erneut.

Single Sign-on und SCIM Enterprise

Anmeldung über Ihren Identitätsanbieter mit SAML 2.0 oder OpenID Connect, auf Wunsch erzwungen. Konten folgen Ihrem Verzeichnis über SCIM 2.0.

Erlaubte Netzwerke Enterprise

Ihre Firma kann den Zugriff auf festgelegte Netzwerke beschränken, für die Console allein oder für Console und App.

Zugriff

Rollen

Rollen in Firma, Teams und Projekten bestimmen, wer welche Aufnahme öffnen darf. Die Console zeigt nie Titel oder Inhalt einer Aufnahme.

Admins

Admins lesen, was mit ihnen geteilt ist, und den Arbeitsbereich eines Teams nur als Mitglied dieses Teams. Der Beitritt steht im Audit-Log.

Zugang für den Support

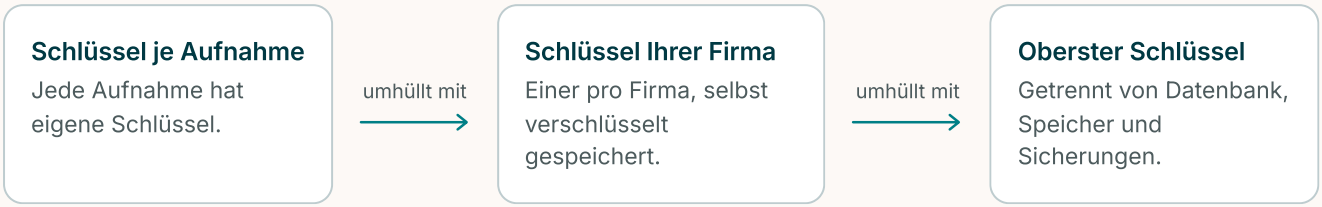
Der Kalima-Support öffnet Ihre Console nur, wenn ein Inhaber oder Admin den Zugang freigibt: nur lesend oder lesend und schreibend, für 24 Stunden bis 7 Tage. Er sieht dabei nie den Inhalt von Aufnahmen.

Zugang zu den Systemen

Der administrative Zugang zu den Systemen ist auf einen kleinen, berechtigten Personenkreis beschränkt und wird protokolliert. Alle Personen mit Zugang sind zur Vertraulichkeit verpflichtet.

3 Verschlüsselung und Trennung

Verschlüsselt vom Gerät bis zur Sicherung, mit eigenen Schlüsseln je Aufnahme.



Wird eine Firma gelöscht, wird ihr Schlüssel vernichtet.

Verschlüsselung

Übertragung

TLS für alle Verbindungen. HSTS ist für zwei Jahre gesetzt, einschließlich aller Subdomains.

Speicherung

Audio wird schon auf dem Gerät verschlüsselt, bevor es hochgeladen wird. Transkripte, Zusammenfassungen und KI-Chats liegen in der Datenbank nur verschlüsselt vor.

Verfahren

AES-256-GCM nach BSI TR-02102-1. Jede Chiffre ist an ihren Ort gebunden. Ein Wert, der zu einem anderen Kunden verschoben wird, lässt sich nicht entschlüsseln.

Schlüssel

Jede Aufnahme hat eigene Schlüssel. Sie sind mit einem Schlüssel Ihrer Firma umhüllt, der selbst verschlüsselt gespeichert ist. Der oberste Schlüssel liegt getrennt von Datenbank, Speicher und Sicherungen.

Trennung

Kunden

Die Daten verschiedener Kunden sind logisch getrennt, jede Firma hat ihren eigenen Schlüssel.

Entwicklung und Produktion

Entwicklung und Produktion laufen auf getrennten Systemen. Tests laufen mit erzeugten Daten, nicht mit Kundendaten.

Datenbank

Die Anwendung greift mit eingeschränkten Rechten auf die Datenbank zu. Die Datenbank ist aus dem Internet nicht erreichbar.

4 Dienstleister, KI und Löschung

Wer Ihre Daten außer Kalima verarbeitet und wann sie gelöscht werden.

Dienstleister und KI

KI-Anfragen

KI-Anfragen gehen nur an Endpunkte in der EU, die nichts speichern. Das ist technisch erzwungen. Der Anbieter der Spracherkennung speichert kein Live-Audio.

Kein KI-Training

Ihre Inhalte werden nicht zum Training von KI-Modellen verwendet.

Unterauftragsverarbeiter

Alle Unterauftragsverarbeiter stehen mit Zweck, Verarbeitungsort und Garantie in Anlage 1 des Vertrags. Änderungen kündigen wir den Inhabern 14 Tage vorher an.

Fehlerberichte

Fehlerberichte enthalten keine Inhalte von Aufnahmen. Passwörter, Zugangsdaten und E-Mail-Adressen werden vor dem Versand entfernt.

Löschung

Aufbewahrungsfrist

Ihre Firma legt fest, ob Aufnahmen nach 30, 90, 180 oder 365 Tagen automatisch gelöscht werden, auf Wunsch nur das Audio.

Papierkorb

Gelöschtes liegt 30 Tage im Papierkorb und wird dann endgültig entfernt. Sicherungskopien sind spätestens sieben Tage danach überschrieben.

Zero Data Retention Enterprise

Gelöschtes ist innerhalb einer Minute endgültig entfernt.

Legal Hold Enterprise

Ein Legal Hold hält das endgültige Löschen für die ganze Firma, für benannte Personen oder für einzelne Projekte an.

Löschung der Firma

Löscht der Inhaber die Firma, werden nach 14 Tagen Widerrufsfrist alle Daten endgültig entfernt. Die Löschung bestätigen wir auf Anfrage in Textform.

5 Protokollierung und Mitbestimmung

Was protokolliert wird und was die Console nie zeigt.

Protokollierung

Audit-Log

Das Audit-Log hält jede Änderung an Ihrer Firma fest: wer, was, wann, von wo und was vorher galt. Auch Änderungen durch Kalima stehen darin. Einträge lassen sich nicht ändern oder löschen.

Aufbewahrung und Export

Gespeichert wird 13 Monate. Sichtbar sind 90 Tage im Team-Plan und 365 Tage im Enterprise-Plan. Export als CSV oder JSON.

Übertragung an Ihr System Enterprise

Laufende Übertragung an Ihr eigenes System über einen signierten HTTPS-Webhook oder einen Splunk HTTP Event Collector.

Anmeldungen

Anmeldungen der letzten 90 Tage je Mitglied, mit Zeit, Methode, Gerät, Land und IP-Adresse. Wer die Ansicht öffnet, steht im Audit-Log.

Beispiel

So liest sich das Audit-Log.

Uhrzeit	Wer	Was
09:12	Anna W.	SSO eingeschaltet
09:40	SCIM	Mitglied über SCIM angelegt
10:05	Lena K.	Freigabe-Richtlinie geändert
11:30	Anna W.	Aufbewahrungsfrist geändert

Für Ihren Betriebsrat

Keine Inhalte in der Console

Die Console zeigt nie Titel oder Inhalt einer Aufnahme.

Keine Auswertung pro Person

Die Nutzung erscheint nur nach Teams und erst ab fünf Personen, nie pro Person.

Merkblatt

Ein druckbares Blatt für Ihren Betriebsrat liegt in der Console.

6 Verfügbarkeit und Betrieb

Wie wir sichern, wiederherstellen, überwachen und Vorfälle melden.

Verfügbarkeit und Wiederherstellung

Datenbank

Fortlaufende Sicherung mit Rückkehr auf jeden Zeitpunkt der letzten sechs Tage, dazu täglich eine Vollsicherung. Sicherungen werden vor dem Hochladen mit AES-256 verschlüsselt.

Wiederherstellung geübt

Die Wiederherstellung wurde am 6. November 2026 geübt und dauerte 61 Sekunden.

Audio

Versionierter Speicher und eine gesperrte Kopie an einem zweiten Standort in Deutschland.

Aktualisierungen

Aktualisierungen laufen ohne Unterbrechung. Der neue Stand wird erst gestartet und geprüft, dann wird umgeschaltet. Schlägt die Prüfung fehl, wird automatisch zurückgerollt.

Überwachung

Erreichbarkeit

Zwei unabhängige Dienste prüfen die Erreichbarkeit von außen. Der Server hält zusätzlich je Minute fest, ob Datenbank und Zwischenspeicher erreichbar waren.

Wächter

Wächter prüfen alle fünf Minuten Datenbank, Speicherplatz und Hintergrundaufgaben. Eine stündliche Probe prüft, ob die Live-Transkription funktioniert.

Bisherige Erreichbarkeit

Vom 31. Juli bis zum 24. November 2026 war die App nach der externen Messung zu 99,99 % erreichbar. Die Messung lief alle drei Minuten und erkannte bis dahin nur Totalausfälle. Aktueller Stand: status.meetkalima.com.

Sicherheitsvorfälle

Ablauf

Für Sicherheitsvorfälle gibt es einen schriftlichen Ablauf: eindämmen, festhalten, Risiko bewerten, entscheiden, melden.

Meldung an Sie

Wird uns eine Verletzung des Schutzes personenbezogener Daten bekannt, melden wir sie Ihnen unverzüglich per E-Mail, mit den Angaben, die Sie für Ihre eigene Meldung nach Art. 33 und 34 DSGVO brauchen.

7 Prüfung und Grenzen

Wie Änderungen und Maßnahmen geprüft werden, und was Kalima nicht macht.

Entwicklung und Schwachstellen

Auslieferung

Jede Änderung läuft durch dieselbe Kette: Bau, automatischer Test gegen eine eigene Testdatenbank, Prüfung der Datenbankänderungen, Start und Prüfung des neuen Stands, Browsertest der Produktion.

Zugangsdaten und Bibliotheken

Jeder Stand wird auf versehentlich eingefügte Zugangsdaten geprüft. Neue Versionen fremder Bibliotheken werden frühestens sieben Tage nach ihrem Erscheinen übernommen.

Schutz der Anwendung

Eine Content Security Policy blockiert fremden Code. Schreibende Anfragen prüfen ihren Ursprung, Schnittstellen sind mengenbegrenzt.

Überprüfung

Regelmäßig

Wir überprüfen diese Maßnahmen zweimal im Jahr und nach jedem Vorfall.

Nachweise und Kontrollen

Auf Anfrage stellen wir die Informationen zum Nachweis unserer Pflichten bereit. Kontrollen durch Sie oder einen zur Verschwiegenheit verpflichteten Prüfer sind nach Vorankündigung möglich.

Was Kalima nicht macht

Damit Sie es vor der Einführung wissen, nicht danach.

Kein zweiter Server in Bereitschaft

Der Dienst läuft auf einem Server. Sicherungen liegen an einem zweiten Ort.

Keine eigenen Schlüssel

Die Schlüssel verwaltet Kalima, einen pro Firma. Schlüssel aus Ihrem eigenen Schlüsseldienst sind nicht möglich.

Nicht jeder Unterauftragsverarbeiter sitzt in der EU

Einige sind US-Unternehmen. Mit ihnen gelten Standardvertragsklauseln.

Kein externer Sicherheitstest bisher

Geprüft wurde intern.

Haben Sie eine Frage zur Sicherheit?

Schreiben Sie uns, auch wenn Sie eine Schwachstelle gefunden haben. Den Vertrag zur Auftragsverarbeitung, die Liste der Unterauftragsverarbeiter und ein Merkblatt für den Betriebsrat finden Sie auch in der Console.

Kontakt		
	E-Mail	security@meetkalima.com
	Sicherheit im Überblick	meetkalima.com/trust
	Auftragsverarbeitung	meetkalima.com/avv
	Aktueller Betriebsstatus	status.meetkalima.com

Kalima ist ein Produkt der ByteHawk GmbH, Fährstraße 217, 40221 Düsseldorf. Dieses Dokument beschreibt den Stand vom 24. November 2026. Wir dürfen die Maßnahmen weiterentwickeln, solange das Schutzniveau nicht sinkt.



Kalima