



Chatline – Security Overview

Stand: März 2026

Vertrauliche B2B-Informationsunterlage. Dieses Dokument gibt Geschäftskunden, Datenschutzverantwortlichen, IT-Verantwortlichen und Procurement-Teams einen Überblick über wesentliche Sicherheits- und Datenschutzmechanismen im Zusammenhang mit der SaaS-Lösung Chatline der HeyHo Systems GmbH.

Dieses Dokument dient der Übersicht und Erläuterung. Verbindlich sind die vertraglichen Vereinbarungen, insbesondere AVV, TOMs, Hauptvertrag und weitere Anlagen. Aus Sicherheitsgründen erhebt dieses Dokument keinen Anspruch auf vollständige Offenlegung sämtlicher operativen Schutzmaßnahmen.

1. Produkt- und Einsatzkontext

- Chatline ist eine cloudbasierte Kommunikationslösung für Unternehmen aus den Bereichen Salon, Beauty, Fitness und Studio. Der Dienst unterstützt insbesondere die automatisierte Kommunikation über WhatsApp und Telefon sowie die Bearbeitung von Termin-, Kurs- und servicebezogenen Anliegen.
- Je nach Konfiguration verarbeitet Chatline insbesondere Kommunikationsinhalte, Transkripte, Gesprächszusammenfassungen, Kontakt- und Vorgangsdaten sowie Portal- und Administrationsdaten.
- Anrufaufzeichnungen werden nicht gespeichert. Sprachverarbeitung erfolgt, soweit technisch vorgesehen, zur Erstellung von Transkripten, Gesprächssteuerung, Zusammenfassungen oder zur Bearbeitung des jeweiligen Anliegens.

2. Sicherheitsgrundsätze

- Zugriff nur nach dem Need-to-know-Prinzip
- Beschränkung von Zugriffen auf berechtigte Personen
- Absicherung von Kommunikationswegen und Systemzugängen
- rollenbasierte Rechtevergabe
- kontrollierte Änderungen an produktiven Systemen
- angemessene Trennung von Mandanten und Umgebungen
- vertraglich geregelter Einsatz von Unterauftragnehmern
- keine Nutzung personenbezogener Kundendaten für eigenes Marketing



-
- keine Nutzung personenbezogener Kundendaten für das Training eigener oder fremder KI-Modelle

3. Zugriffsschutz und Berechtigungen

- Zugriffe auf produktive Systeme und personenbezogene Daten sind auf berechtigte Personen beschränkt. Berechtigungen werden rollenbezogen und nach dem Erforderlichkeitsprinzip vergeben.
- Administrative, betriebliche und supportbezogene Zugriffe erfolgen nur, soweit dies für Betrieb, Sicherheit, Support, Fehleranalyse oder die Erfüllung vertraglicher Pflichten erforderlich ist.
- Zugangsdaten und vergleichbare Geheimnisse werden geschützt verwaltet. Für besonders schutzrelevante oder administrative Zugriffe werden angemessene zusätzliche Schutzmaßnahmen eingesetzt.

4. Infrastruktur und Hosting

- Chatline wird unter Einsatz externer technischer Dienstleister betrieben. Je nach Funktionsbereich können hierzu insbesondere Kommunikationsdienste, Hosting- und Cloud-Infrastrukturdienste, KI- und Sprachverarbeitungsdienste sowie Monitoring- und Betriebsdienste gehören.
- Die jeweils eingesetzten Unterauftragnehmer sind in der aktuellen Subprozessorenliste dokumentiert. Hosting- und Infrastrukturleistungen können über etablierte Cloud- und Plattformanbieter erbracht werden.

5. Datenübertragung und Geheimnisschutz

- Elektronische Datenübertragungen erfolgen über abgesicherte Verbindungen. Zugangsschlüssel, Tokens, API-Credentials und vergleichbare Geheimnisse werden gesondert geschützt und auf berechnete Stellen beschränkt.
- Soweit angemessen und vorgesehen, werden gespeicherte Daten oder sicherheitsrelevante Geheimnisse verschlüsselt oder durch gleichwertige Maßnahmen geschützt.

6. Mandantentrennung und Umgebungen

- Daten verschiedener Kunden werden logisch voneinander getrennt verarbeitet, soweit mehrere Kunden auf derselben Plattform betrieben werden. Entwicklungs-, Test- und Produktivumgebungen werden organisatorisch und soweit möglich technisch voneinander getrennt.
- Der Einsatz produktiver personenbezogener Daten in Test- oder Entwicklungsumgebungen erfolgt nur ausnahmsweise, soweit erforderlich, angemessen abgesichert und datenschutzrechtlich zulässig.

7. Logging, Monitoring und Nachvollziehbarkeit

- Zur Sicherstellung von Stabilität, Sicherheit, Fehleranalyse und Missbrauchserkennung können technische Ereignisse, Betriebszustände, Fehlerzustände oder sicherheitsrelevante Vorgänge



protokolliert werden. Soweit technisch vorgesehen, können administrative Änderungen oder Supportzugriffe nachvollziehbar dokumentiert werden.

- Protokollierungsdaten werden gegen unberechtigten Zugriff geschützt und nicht für vertragsfremde Zwecke verwendet.

8. Support und Wartung

- Support- und Wartungszugriffe erfolgen nur im erforderlichen Umfang und ausschließlich durch berechtigte Personen. Soweit technisch vorgesehen, können solche Zugriffe dokumentiert oder nachvollzogen werden.
- Personenbezogene Daten aus Support- oder Wartungskontexten werden nicht für eigene Zwecke genutzt.

9. Verfügbarkeit, Resilienz und Wiederherstellung

- HeyHo Systems betreibt Chatline mit dem Ziel einer hohen Verfügbarkeit und Belastbarkeit. Gleichwohl kann eine jederzeit ununterbrochene Verfügbarkeit nicht garantiert werden.
- Es bestehen Maßnahmen zur Erkennung und Behandlung technischer Störungen. Soweit erforderlich, werden Datensicherungen, Wiederherstellungsmechanismen, Redundanzen oder sonstige organisatorische und technische Maßnahmen eingesetzt, um die Kontinuität des Betriebs angemessen abzusichern.

10. Incident Management und Datenschutzverletzungen

- HeyHo Systems unterhält Prozesse zur Erkennung, Bewertung, Behandlung und Nachverfolgung von Sicherheitsvorfällen und Datenschutzverletzungen.
- Relevante Datenschutzverletzungen im Zusammenhang mit der Auftragsverarbeitung werden dem jeweiligen Kunden unverzüglich nach Maßgabe der vertraglichen Vereinbarungen mitgeteilt. Informationen werden, soweit verfügbar, schrittweise ergänzt.

11. Unterauftragnehmer und Drittlandbezüge

- HeyHo Systems setzt Unterauftragnehmer nur ein, soweit diese für die Leistungserbringung erforderlich sind und hinreichende Garantien für eine datenschutzgerechte Verarbeitung bieten. Unterauftragnehmer werden vertraglich eingebunden.
- Soweit einzelne Dienste Drittlandbezüge haben können, insbesondere in die USA, erfolgt dies nur unter Beachtung der gesetzlichen Anforderungen, insbesondere auf Grundlage geeigneter Garantien wie Angemessenheitsbeschlüssen, Standardvertragsklauseln oder sonstigen zulässigen Mechanismen.



12. Datenschutz und Rollenverständnis

- Soweit HeyHo Systems personenbezogene Daten im Auftrag von Geschäftskunden verarbeitet, erfolgt dies auf Grundlage des jeweiligen Auftragsverarbeitungsvertrags. Die konkreten technischen und organisatorischen Maßnahmen ergeben sich aus den jeweils aktuellen TOMs.
- Die öffentliche Datenschutzerklärung von HeyHo Systems regelt ergänzend die Verarbeitung personenbezogener Daten in den Fällen, in denen HeyHo Systems selbst datenschutzrechtlich verantwortlich ist.

13. Kundenseitige Mitwirkung und Shared Responsibility

- Der sichere und rechtskonforme Betrieb von Chatline setzt auch eine angemessene Mitwirkung des Kunden voraus. Hierzu gehören insbesondere die Verwaltung von Zugangsrechten, der Schutz eigener Zugangsdaten, die rechtmäßige Konfiguration von Kommunikationsprozessen sowie die Prüfung, ob die Nutzung der Dienste den eigenen fachlichen und regulatorischen Anforderungen entspricht.
- Soweit der Kunde selbst Drittanbieter, Kommunikationskanäle, Vorlagen, Inhalte, Integrationen oder Administratoren verwaltet, liegt die Verantwortung für diese kundenseitigen Bereiche beim Kunden.

14. Löschkonzept und Speicherlogik

- Personenbezogene Daten werden nur so lange verarbeitet und gespeichert, wie dies für die vertraglich vorgesehenen Zwecke, den sicheren Betrieb, die Einhaltung gesetzlicher Pflichten oder berechtigte Gründe zur befristeten Aufbewahrung erforderlich ist.
- Details zu Löschlogik, Speicherbegrenzung und Vertragsbeendigung ergeben sich aus dem AVV, den TOMs, dem Hauptvertrag sowie internen Löscho- und Aufbewahrungsprozessen.

15. Grenzen dieses Dokuments

- Dieses Security Overview ist eine zusammenfassende Informationsunterlage. Es ersetzt keine individuelle rechtliche Prüfung, keine Security Due Diligence und keine verbindlichen vertraglichen Zusagen außerhalb der ausdrücklich vereinbarten Dokumente.
- Verbindlich sind insbesondere Hauptvertrag bzw. SaaS-Nutzungsbedingungen, Auftragsverarbeitungsvertrag, TOMs, aktuelle Subprozessorenliste sowie etwaige individuelle Vereinbarungen.