ANLAGE 2 ZUM AUFTRAGSVERARBEITUNGSVERTRAG

Technische und organisatorische Maßnahmen der HeyVera GmbH

Fassung	v2
Datum der Fassung	12. Oktober 2026
Wirksam ab	11. November 2026
Anbieter	HeyVera GmbH, Dresdener Straße 113b, 10179 Berlin

Anlage zum Auftragsverarbeitungsvertrag zwischen der HeyVera GmbH, Dresdener Straße 113b, 10179 Berlin, und dem Kunden

Fassung vom 12. Oktober 2026, wirksam ab 11. November 2026

HeyVera verarbeitet personenbezogene Daten im Auftrag des Kunden auf ihrer Plattform. Die Plattform umfasst die KI-Telefonassistenz Vera und das Kundenportal. Diese Anlage beschreibt die dabei eingesetzten technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO. Die Abschnitte 1 bis 8 beschreiben die Maßnahmen im Betrieb der Plattform. Die Abschnitte 9 bis 13 beschreiben die organisatorischen Maßnahmen im Team von HeyVera. Die Anlage gibt den nachweisbaren Stand zum Tag ihres Inkrafttretens wieder. Die Maßnahmen der Unterauftragsverarbeiter gelten ergänzend nach ihren Auftragsverarbeitungsverträgen.

Die jeweils aktuelle Fassung dieser Anlage ist unter https://www.heyvera.de/avv abrufbar. Änderungen richten sich nach § 8 Abs. 2 i.V.m. § 18 Abs. 3 des Auftragsverarbeitungsvertrags.

1. Authentifizierung und Berechtigungsmanagement

Die Plattform verlangt für die geschützten Seiten des Kundenportals eine Anmeldung. Der Anmeldedienst prüft die Sitzung bei jedem Seitenaufruf. Gesperrte Benutzerkonten erhalten keinen Zugang.

Das Portal ordnet jedes Benutzerkonto einem oder mehreren Mandanten und einer Rolle zu. Die Rollen „Inhaber“, „Administrator“ und „Mitglied“ steuern die Rechte. Inhaber und Administratoren dürfen Mitglieder einladen und Konfigurationen verwalten. Mitglieder erhalten Leserechte und die Rechte, die eine einzelne Funktion vorsieht. Die Datenbank prüft bei Kundenkonten zusätzlich die Benutzerkennung, den Mandanten und die Rolle.

2. Verschlüsselung bei Übertragung und Speicherung

Supabase überträgt Daten über TLS 1.2 und verschlüsselt Datenträger sowie Backups mit AES-256. Google Cloud verschlüsselt Kundendaten nach Abschnitt 7.1.1 seines Auftragsverarbeitungsvertrags. Die Anbieter verwalten die dafür eingesetzten Schlüssel.

Die Plattform verschlüsselt Zugangsdaten zu angebundenen Verwaltungssystemen vor der Speicherung mit AES-256-GCM. Den Schlüssel und die Zugangsdaten zu weiteren Diensten legt HeyVera im Secret Manager von Google Cloud ab. Die Dienste erhalten diese Secrets erst zur Laufzeit über ihre jeweilige Dienstkennung.

3. Mandantentrennung

Die Datenbank ordnet die Bestände über eine Mandantenkennung dem jeweiligen Kunden zu. Row Level Security, eine Zugriffskontrolle auf Zeilenebene, lässt angemeldete Kundenkonten nur auf Zeilen ihres Mandanten zugreifen. Die Datenbank setzt diese Grenze unabhängig von der Oberfläche durch.

Der Sprachdienst und die Auswertungsläufe erhalten die Mandantenkennung für den jeweiligen Verarbeitungsschritt. Abschnitt 8 beschreibt die technischen Zugänge von HeyVera.

4. Protokollierung von Zugriffen und Änderungen

Die Datenbank protokolliert das Anlegen, Ändern und Löschen von Mandanten, Sprachassistenten, Assistentenkonfigurationen, Funktionsfreigaben, Anbindungen und Benutzerrollen. Jeder Eintrag enthält den betroffenen Datensatz, den Zeitpunkt, die geänderten Felder und, soweit der Zugriff über ein Benutzerkonto erfolgt, die Benutzerkennung. Die Protokollierung entfernt Zugangsdaten aus den gespeicherten alten und neuen Werten. Kundenkonten können diese Einträge nicht ändern oder löschen.

Die Plattform protokolliert für Gesprächsaufzeichnungen Wiedergaben, Downloads, fehlgeschlagene Zugriffe und Löschvorgänge mit Benutzerkennung, Zeitpunkt und Ergebnis. Das interne Administrationswerkzeug protokolliert den handelnden Superadmin bei jedem Aufruf. Beim Abruf eines Transkripts hält es zusätzlich Mandant und Gespräch fest.

5. Backup und Wiederherstellung

Supabase erstellt nach seiner vertraglichen Zusage täglich verschlüsselte Backups auf unabhängigen Speichersystemen. Google Cloud sagt in Abschnitt 7.1.1 seines Auftragsverarbeitungsvertrags zu, den Zugang zu Kundendaten nach einem Vorfall wiederherzustellen. Backup und Recovery der Plattformdaten liegen bei diesen Anbietern.

6. Löschprozesse

Der Kunde kann die Löschung einer betroffenen Person über die Löschfunktion im Portal veranlassen. Die Plattform entfernt dabei die Person, ihre Anrufprotokolle, Tickets und zugehörige abgeglichene Datensätze.

Gesprächsaufzeichnungen sind im Auslieferungszustand ausgeschaltet. Aktiviert der Kunde die Funktion, setzt die Plattform beim Anlegen der Aufzeichnung einen Löschzeitpunkt. Die Frist beträgt 30 Tage, soweit nichts anderes vereinbart ist. Die Plattform löscht fällige Aufzeichnungen stündlich automatisch und protokolliert jede Löschung. Audio, das die Plattform nur für die nachgelagerte Umwandlung in Text zwischenspeichert, löscht die Plattform nach dem Umwandlungsversuch, spätestens 24 Stunden nach dem Speichern.

7. Incident Management

Sentry erfasst technische Fehler der Anwendung und des Sprachdienstes. Die Plattform übermittelt an Sentry keine Benutzerkennungen. Telefonnummern und E-Mail-Adressen entfernt die Plattform vor der Übermittlung aus den Fehlerdaten; die Rufnummer des Anrufs erscheint höchstens gekürzt auf die ersten vier Zeichen. Aufzeichnungen von Sitzungen im Kundenportal zeigen keine Texte und keine Medien. Google Cloud Monitoring prüft die Erreichbarkeit und technische Grenzwerte, darunter Fehlerraten und Auslastung. Für die hinterlegten Empfänger erzeugt die Plattform Benachrichtigungen aus diesen Regeln.

8. Zugriff durch HeyVera und eingesetzte Unterauftragsverarbeiter

HeyVera kann Kundendaten über gesonderte Superadmin-Konten mandantenübergreifend abrufen und bearbeiten. Der Zugang setzt ein angemeldetes Benutzerkonto und eine gesonderte Freischaltung durch HeyVera voraus. Dienste von HeyVera greifen mit technischen Dienstkonten auf die Daten zu, soweit sie Anrufe bearbeiten, Inhalte auswerten, Anbindungen synchronisieren oder den Betrieb sichern.

Die Unterauftragsverarbeiter erhalten Daten für ihren jeweiligen Verarbeitungsschritt. Google Cloud und Supabase betreiben die Anwendung, Datenbank, Anmeldung und Dateispeicher. Telnyx und, bis zum Abschluss der Umstellung, Twilio transportieren Telefonate. Lettermint versendet transaktionale E-Mails. Deepgram, AssemblyAI und ElevenLabs verarbeiten Sprache. OpenAI und Anthropic über Google Vertex AI verarbeiten Text für Gesprächsführung, Auswertung oder die Chat-Funktion. Sentry erhält technische Fehlerdaten. Je nach gebuchter oder aktivierter Funktion kommen Meta für WhatsApp, PostHog für die Portal-Analyse und die Browser-Push-Dienste hinzu.

Lettermint verarbeitet die transaktionalen E-Mails in den Niederlanden innerhalb der Europäischen Union; Backups liegen in Deutschland.

Die Anlage „Unterauftragsverarbeiter der HeyVera GmbH“ nennt Rechtsträger, Verarbeitungsorte, Drittlandgarantien und Verträge. Sie kennzeichnet auch Dienste, die als eigenständig Verantwortliche handeln.

9. Vertraulichkeit und Unterweisung

HeyVera gewährt Zugriff auf Kundendaten nur Personen, die vor dem ersten Zugriff eine Verpflichtung zur Vertraulichkeit unterschrieben haben. Die Verpflichtung gilt nach dem Ende ihrer Tätigkeit für HeyVera fort. HeyVera führt eine Liste der Personen, die Zugriff auf Kundendaten haben.

HeyVera unterweist die Personen auf dieser Liste in Datenschutz und Datensicherheit. Personen, die neu Zugriff erhalten, unterweist HeyVera vor dem ersten Zugriff auf Kundendaten. HeyVera wiederholt die Unterweisung mindestens einmal im Jahr. HeyVera dokumentiert jede Unterweisung mit Datum und Teilnehmenden.

10. Berechtigungen und Mehrfaktor-Anmeldung

HeyVera führt eine Übersicht der Zugänge zu den Diensten, über die Kundendaten erreichbar sind. Die Übersicht nennt je Dienst die Personen mit Zugang und deren Berechtigung.

HeyVera entzieht oder ändert Berechtigungen ohne unangemessene Verzögerung, wenn eine Person ihre Rolle wechselt oder ausscheidet, und dokumentiert jede Änderung und jeden Entzug.

Persönliche Zugänge von HeyVera mit Administrationsrechten bei den Unterauftragsverarbeitern setzen eine Mehrfaktor-Anmeldung voraus.

HeyVera prüft die vergebenen Berechtigungen anhand der Übersicht mindestens einmal im Jahr. HeyVera protokolliert jede Prüfung mit Datum, Ergebnis und den daraus folgenden Änderungen.

11. Homeoffice, mobile Arbeit und Endgeräte

Personen, die im Homeoffice oder mobil auf Kundendaten zugreifen, beachten eine verbindliche Regel von HeyVera für ihre Endgeräte. Die Festplatte des Geräts ist verschlüsselt. Das Gerät sperrt den Bildschirm automatisch, wenn es nicht benutzt wird. Die Regel untersagt, Kundendaten lokal auf dem Gerät abzulegen.

HeyVera prüft für jede Person auf der Liste nach Abschnitt 9, dass ihre Geräte diese Regel einhalten, und dokumentiert das Ergebnis.

12. Ablauf bei Datenschutzverletzungen

HeyVera hat einen dokumentierten Ablauf für Verletzungen des Schutzes personenbezogener Daten. Der Ablauf regelt die Erkennung, die Bewertung und die Benachrichtigung des Kunden nach § 10 Abs. 3 bis 5 des Auftragsverarbeitungsvertrags. Er benennt die zuständigen Personen, ihre Vertretung und die Kontaktwege. HeyVera hat den Ablauf in einer Übung durchgespielt und das Ergebnis dokumentiert.

Sobald eine Verletzung, die Daten des Kunden betrifft, anhand objektiver Umstände festgestellt ist, informiert HeyVera den Kunden unverzüglich. Fehlende Angaben liefert HeyVera nach.

13. Test der Wiederherstellung

HeyVera testet die Wiederherstellung der Plattformdaten aus einem Backup. HeyVera dokumentiert für jeden Test das Ergebnis, die Dauer und die Behebung aufgetretener Fehler. Der Test ergänzt die Zusagen der Anbieter aus Abschnitt 5.