

Technische und organisatorische Maßnahmen der HeyVera GmbH

Fassung	v1
Datum der Fassung	8. Oktober 2026
Wirksam ab	12. Oktober 2026
Gültig bis	10. 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

Stand 8. Oktober 2026

HeyVera verarbeitet personenbezogene Daten im Auftrag des Kunden auf ihrer Plattform. Die Plattform umfasst die KI-Telefonassistentin Vera und das Kundenportal. Diese Anlage beschreibt die dabei eingesetzten technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO. Sie gibt den nachweisbaren Stand zum genannten Datum 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 Löschezitpunkt. 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.