Master Data Processing Agreement (MDPA)

Effective date: 2026-02-08

Legal version: 2026-02-08

Legal entity: voice2evolve UG (haftungsbeschränkt)

Registered office: Amtsgericht Stuttgart, HRB 803557

Translation notice: This is a German translation provided for convenience. The English version prevails in case of discrepancy.

Hinweis: Diese deutsche Fassung dient der Information. Im Falle von Abweichungen gilt die englische Fassung.

Dieses Master-Datenverarbeitungsaddendum („MDPA“) wird durch Verweis Bestandteil der Vereinbarung über die Nutzung der Voice2Evolve-Dienste („Vereinbarung“), die zwischen Ihnen, dem Kunden (wie in der Vereinbarung definiert) („Kunde“), und **Voice2Evolve UG (haftungsbeschränkt)** („Voice2Evolve“) geschlossen wird, um die Vereinbarung der Parteien hinsichtlich der Verarbeitung personenbezogener Daten durch Voice2Evolve ausschließlich im Auftrag des Kunden abzubilden. Beide Parteien werden gemeinsam als „Parteien“ und jeweils einzeln als „Partei“ bezeichnet.

Sofern in diesem MDPA nichts anderes bestimmt ist, bleiben die Bestimmungen der Vereinbarung in vollem Umfang in Kraft. Großgeschriebene Begriffe, die in diesem MDPA nicht definiert sind, haben die in der Vereinbarung festgelegte Bedeutung. Etwaige zuvor zwischen Voice2Evolve und dem Kunden getroffene datenschutzrechtliche Regelungen oder Vereinbarungen werden durch dieses MDPA ersetzt.

Dieses MDPA trat ursprünglich am 08.02.2026 in Kraft und wurde zuletzt am 13. März 2026 aktualisiert. Es gilt zwischen dem Kunden und Voice2Evolve ab dem Wirksamkeitsdatum der Vereinbarung („MDPA-Wirksamkeitsdatum”).

Die Parteien vereinbaren Folgendes: (MDPA)

1. Begriffsbestimmungen

Um eine Detailtiefe vergleichbar mit führenden Rahmenwerken zu erreichen, definiert dieser Abschnitt zentrale Begriffe wie „Genehmigte Rechtsordnung“, „Besondere Kategorien personenbezogener Daten“, „Standardvertragsklauseln“

und „Aufsichtsbehörde“, um Klarheit und eine umfassende Ausrichtung an der DSGVO und verwandten Regelungen sicherzustellen.

Soweit hierin nicht anders definiert, haben großgeschriebene Begriffe die in den anwendbaren Datenschutzgesetzen festgelegte Bedeutung.

- **Affiliate (verbundenes Unternehmen):** Jede Einheit, die eine Partei direkt oder indirekt beherrscht, von ihr beherrscht wird oder unter gemeinsamer Beherrschung steht.
- **Approved Jurisdiction (genehmigte Rechtsordnung):** Jeder Staat innerhalb des EWR oder solche Staaten, denen die Europäische Kommission ein angemessenes Schutzniveau bescheinigt.
- **Controller (Verantwortlicher):** Die Stelle, die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.
- **Processor (Auftragsverarbeiter):** Die Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.
- **Personal Data (personenbezogene Daten):** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- **Processing (Verarbeitung):** Jeder Vorgang im Zusammenhang mit personenbezogenen Daten, z. B. Erhebung, Speicherung, Veränderung, Übermittlung oder Löschung.
- **Subprocessor (Unterauftragsverarbeiter):** Ein von Voice2Evolve eingesetzter Dritter als Auftragsverarbeiter.
- **Data Subject (betroffene Person):** Eine identifizierbare natürliche Person, auf die sich die personenbezogenen Daten beziehen.
- **Security Measures (Sicherheitsmaßnahmen):** Die von Voice2Evolve implementierten technischen und organisatorischen Maßnahmen gemäß Anlage A.
- **Data Breach (Datenschutzverletzung):** Ein Sicherheitsvorfall, der zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt.
- **Supervisory Authority (Aufsichtsbehörde):** Eine unabhängige öffentliche Stelle gemäß Art. 51 DSGVO.
- **Special Categories of Personal Data (besondere Kategorien personenbezogener Daten):** Wie in Art. 9 DSGVO definiert, einschließlich Gesundheits-, biometrischer oder strafrechtlicher Daten.
- **Data Protection Laws (Datenschutzgesetze):** DSGVO, UK GDPR und CPRA gemeinsam.

---

2. Rollen und Verantwortlichkeiten

2.1 Verhältnis der Parteien

Der Kunde handelt als **Verantwortlicher**, Voice2Evolve handelt als **Auftragsverarbeiter**.

2.2 Weisungen des Kunden

Voice2Evolve verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisungen des Kunden. Wenn Voice2Evolve der Auffassung ist, dass eine Weisung gegen die DSGVO oder anwendbares Recht verstößt, informiert Voice2Evolve den Kunden unverzüglich.

2.3 Umfang und Zweck

Die Verarbeitung umfasst KI-basiertes Voice-Sparring, Transkription, Scoring und zugehörige Analysen.

2.4 Dauer

Die Verarbeitung erfolgt für die Laufzeit der Vereinbarung und endet, wenn alle Daten gemäß Abschnitt 15 zurückgegeben oder gelöscht wurden.

2.5 Besondere Kategorien und Sprachdaten

Die Leistungen verarbeiten Sprachaufnahmen zum Zweck des KI-gestützten Gesprächstrainings (Sparring) und der Analyse. Voice2Evolve verarbeitet Sprachdaten nicht zum Zweck der eindeutigen Identifizierung einer natürlichen Person (biometrische Identifizierung) im Sinne von Art. 9 Abs. 1 DSGVO. Sprachaufnahmen, die im Rahmen dieses MDPA verarbeitet werden, werden daher nicht als besondere Kategorien personenbezogener Daten behandelt. Der Kunde darf keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) in die Dienste einbringen, sofern dies nicht ausdrücklich schriftlich vereinbart wurde.

2.6 Automatisierte Entscheidungsfindung

Die Dienste erzeugen Bewertungen, Analysen und Feedback mittels KI-Modellen. Diese Ergebnisse dienen ausschließlich Informations- und Übungszwecken und entfalten keine rechtlichen Wirkungen oder ähnlich erhebliche Auswirkungen auf betroffene Personen im Sinne von Art. 22 Abs. 1 DSGVO. Es werden keine Entscheidungen mit rechtlicher oder vergleichbarer Wirkung allein auf Grundlage automatisierter Verarbeitung getroffen.

2.7 Mandantendatentrennung

Voice2Evolve garantiert vertraglich die logische Trennung der personenbezogenen Daten jedes Kunden von denen anderer Kunden. Die Isolation wird durch Row-Level-Security-Richtlinien auf Datenbankebene, mandantenspezifische Authentifizierung und anwendungsseitige Zugriffskontrollen durchgesetzt. Personenbezogene Daten eines Kunden werden nicht mit denen eines anderen Kunden vermischt oder diesem zugänglich gemacht.

2.8 Datenschutz-Kontakt

Der benannte Ansprechpartner für alle Datenschutzangelegenheiten nach diesem MDPA ist: **Voice2Evolve UG (haftungsbeschränkt)** — E-Mail: privacy@voice2evolve.com

---

3. Pflichten des Verantwortlichen (Kunde)

Der Kunde informiert Voice2Evolve unverzüglich über Beschwerden, Anfragen oder Untersuchungen betroffener Personen oder einer Aufsichtsbehörde, die die Verarbeitung nach diesem MDPA betreffen. Beide Parteien arbeiten zusammen, um eine konsistente und fristgerechte Kommunikation mit Behörden und betroffenen Personen sicherzustellen.

Der Kunde:

- stellt eine Rechtsgrundlage für alle bereitgestellten Daten sicher,
- erfüllt Informations- und Einwilligungspflichten gegenüber betroffenen Personen,
- stellt korrekte, minimierte Daten bereit,
- dokumentiert seine Verarbeitungszwecke und informiert Voice2Evolve über Änderungen.

---

4. Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 lit. a–h DSGVO) und rechtsgebietsübergreifende Compliance

Voice2Evolve hält auch gleichwertige Pflichten als Auftragsverarbeiter nach US-Bundesstaaten-Datenschutzgesetzen ein, einschließlich CPRA (Kalifornien) und CDPA (Virginia), um die gleichen Datenschutz-, Vertraulichkeits- und Betroffenenrechte-Grundsätze über Rechtsordnungen hinweg konsistent anzuwenden.

Voice2Evolve wird:

1. personenbezogene Daten ausschließlich auf schriftliche Weisung des Kunden verarbeiten,
2. die Vertraulichkeit des Personals sicherstellen (Art. 28 Abs. 3 lit. b DSGVO),
3. geeignete technische und organisatorische Maßnahmen umsetzen (Art. 28 Abs. 3 lit. c DSGVO),
4. die Autorisierung von Unterauftragsverarbeitern beachten und eine aktuelle Liste führen (Art. 28 Abs. 3 lit. d DSGVO),
5. den Kunden bei der Beantwortung von Betroffenenanfragen unterstützen (Art. 28 Abs. 3 lit. e DSGVO),
6. den Kunden bei DSFA/DPIA und Konsultationen mit Aufsichtsbehörden unterstützen (Art. 28 Abs. 3 lit. f DSGVO),
7. Daten nach Beendigung löschen oder zurückgeben, sofern keine gesetzliche Pflicht entgegensteht (Art. 28 Abs. 3 lit. g DSGVO),
8. alle Informationen zur Verfügung stellen, die zur Nachweisführung erforderlich sind, und eine Verifikation gemäß Abschnitt 10 unterstützen (Art. 28 Abs. 3 lit. h DSGVO),
9. mit Aufsichtsbehörden kooperieren,
10. Verzeichnisse von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO führen.

---

5. Unterauftragsverarbeitung

Voice2Evolve kann Unterauftragsverarbeiter gemäß Anlage B einsetzen. Alle Unterauftragsverarbeiter werden durch schriftliche Verträge mit Datenschutzpflichten gebunden, die den in diesem MDPA festgelegten Pflichten gleichwertig sind. Voice2Evolve bleibt für Handlungen und Unterlassungen seiner Unterauftragsverarbeiter verantwortlich.

5.1 Vorankündigung neuer Unterauftragsverarbeiter

Voice2Evolve informiert den Kunden mindestens dreißig (30) Kalendertage vor der Autorisierung eines neuen Unterauftragsverarbeiters zur Verarbeitung personenbezogener Daten. Die Benachrichtigung erfolgt über die im Kundenkonto hinterlegten Kontaktdaten oder über einen Änderungsbenachrichtigungsmechanismus, den der Kunde abonnieren kann.

5.2 Widerspruchsrecht

Der Kunde kann innerhalb der dreißigtägigen Ankündigungsfrist aus berechtigten datenschutzrechtlichen Gründen schriftlich Widerspruch gegen einen neuen Unterauftragsverarbeiter einlegen. Voice2Evolve unternimmt wirtschaftlich zumutbare Anstrengungen, den Widerspruch auszuräumen, einschließlich durch Angebot eines alternativen Unterauftragsverarbeiters oder einer alternativen Konfiguration. Kann Voice2Evolve den Widerspruch nicht innerhalb von dreißig (30) Tagen nach Erhalt angemessen berücksichtigen, kann der Kunde die

betroffenen Leistungen — oder, sofern der Unterauftragsverarbeiter für den gesamten Dienst wesentlich ist, die Vereinbarung — ohne Vertragsstrafe durch schriftliche Mitteilung vor Beginn der Verarbeitung durch den neuen Unterauftragsverarbeiter kündigen.

---

6. Sicherheitsmaßnahmen (Art. 32 DSGVO)

Das Sicherheitsrahmenwerk von Voice2Evolve umfasst u. a. detaillierte **Richtlinien zum Management von Verschlüsselungsschlüsseln**, die sicherstellen, dass Schlüssel gemäß ISO 27001 und NIST SP 800-57 erzeugt, gespeichert, rotiert und vernichtet werden. Schlüssel werden niemals fest im Code hinterlegt oder im Klartext gespeichert; der Zugriff auf Schlüsselmaterial ist streng beschränkt.

Voice2Evolve unterhält eine formale **Incident-Response-Richtlinie** mit dokumentierten Verfahren zur schnellen Erkennung, Untersuchung, Eskalation und Eindämmung von Sicherheitsereignissen gemäß anwendbaren Datenschutzgesetzen.

Zusätzlich wendet Voice2Evolve **Pseudonymisierungsstandards** für sämtliche Analyse- und Transkriptionsdaten an, um eine direkte Identifizierung betroffener Personen zu verhindern. Pseudonymisierte Kennungen werden zufällig generiert und getrennt von Kontoinformationen gespeichert, um Art. 32 Abs. 1 lit. a DSGVO (Vertraulichkeit und Belastbarkeit) zu erfüllen.

Voice2Evolve setzt die in **Anlage A** beschriebenen Sicherheitsmaßnahmen um, insbesondere:

- Verschlüsselung ruhender und übertragener Daten,
- rollenbasierte Zugriffskontrolle nach dem Prinzip der geringsten Rechte,
- Multifaktor-Authentifizierung,
- Protokollierung, Monitoring und Incident-Management,
- regelmäßige Schwachstellenanalysen und Sicherheitstests entsprechend dem Risiko,
- sichere Löschung und 30-Tage-Aufbewahrungsrichtlinie.

---

7. Meldung von Datenschutzverletzungen (Art. 33 DSGVO)

Voice2Evolve informiert den Kunden über jede Verletzung des Schutzes personenbezogener Daten unverzüglich und spätestens innerhalb von zweiundsiebzig (72) Stunden nach Kenntniserlangung. Die Erstmitteilung enthält, soweit zum Zeitpunkt der Mitteilung vernünftigerweise verfügbar, die Art der Verletzung, die Kategorien und ungefähre Zahl betroffener Personen und Datensätze, die wahrscheinlichen Folgen sowie die getroffenen oder

vorgeschlagenen Maßnahmen zur Behebung. Soweit vollständige Angaben innerhalb des Benachrichtigungszeitraums noch nicht vorliegen, stellt Voice2Evolve die verbleibenden Informationen phasenweise ohne weitere unangemessene Verzögerung bereit.

8. Rechte betroffener Personen

Verifizierung der Identität betroffener Personen

Vor Erfüllung einer Betroffenenanfrage verifiziert Voice2Evolve die Identität des Anfragenden gemäß Art. 12 Abs. 6 DSGVO. Verifizierungsmethoden können die Authentifizierung über registrierte Kontodaten oder andere angemessene Verfahren umfassen, um unbefugten Zugriff oder unbefugte Offenlegung zu verhindern (Art. 15–22 DSGVO).

Voice2Evolve unterstützt den Kunden bei der Erfüllung von Anträgen auf Auskunft, Berichtigung, Einschränkung, Löschung, Datenübertragbarkeit oder Widerspruch. Bei Anfragen zur Datenübertragbarkeit stellt Voice2Evolve die betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format (JSON oder CSV) bereit. Voice2Evolve beantwortet Anfragen betroffener Personen nicht direkt, sofern es nicht vom Kunden dazu autorisiert ist.

---

9. Internationale Datenübermittlungen (Art. 44–49 DSGVO)

Im Einklang mit Leitlinien des Europäischen Datenschutzausschusses (EDPB) führt Voice2Evolve vor internationalen Datenübermittlungen **Transfer Impact Assessments (TIAs)** durch, um rechtliche und praktische Schutzmaßnahmen im Empfängerland zu bewerten (u. a. Überwachungsgesetze, behördliche Zugriffe, Rechtsbehelfe).

Die entsprechenden TIAs werden als Teil des internen Vendor-Registers und der Vendor-Sicherheitsbewertungen geführt. Relevante Drittlandübermittlungen sowie direkte Unterauftragsverarbeiter mit dokumentierten Weiterübermittlungen werden jeweils gesondert bewertet.

- **Supabase Inc.** — Die primäre Projektregion ist die EU (Stockholm, Schweden). Zusätzlich dokumentiert Supabase in DPA und TIA Weiterübermittlungen an Unterauftragsverarbeiter in den Vereinigten Staaten und Singapur für Support, Observability und ergänzende Tooling-Dienste. Die Übermittlungen stützen sich auf SCCs und ergänzende Schutzmaßnahmen gemäß Supabase-DPA und Supabase-TIA. TIA vorhanden: *Supabase Vendor Security Assessment (2026-03-02)* und *Supabase Transfer Impact Assessment (2025-03-14)*.

- **OpenAI, L.L.C.** — SCCs (EU-Kommissionsbeschluss 2021/914, Modul 2) + CPRA-Compliance + EU-US DPF-Teilnahme. Voice2Evolve pflegt eine Zero-Data-Retention-(ZDR-)API-Konfiguration und wird diese ohne vorherige schriftliche Mitteilung an betroffene Kunden nicht herabstufen oder deaktivieren. TIA vorhanden: *OpenAI Vendor Security Assessment (2026-03-02)*.
- **Anthropic PBC** — SCCs + CPRA-Compliance. Datenminimierung angewandt; Verwendung ausschließlich zur Qualitätsbewertung. TIA vorhanden: *Anthropic Vendor Security Assessment (2026-03-02)*.
- **Stripe Payments Europe Ltd.** — Primäre Entität in der EU; US-Entität abgedeckt durch SCCs + PCI DSS Level 1. TIA vorhanden: *Stripe Vendor Security Assessment (2026-03-02)*.
- **Vercel Inc.** — SCCs; EU-Region-Deployment verfügbar und für EWR-Traffic genutzt. TIA vorhanden: *Vercel Vendor Security Assessment (2026-02-10)*.
- **Cloudflare, Inc.** — SCCs + EU-US DPF. Verarbeitung beschränkt auf DNS-Auflösung und transientes verschlüsseltes WebRTC-Relay (DTLS-SRTP); kein Zugriff auf Anwendungsschichtinhalte. TIA vorhanden: *Cloudflare Vendor Security Assessment (2026-02-10)*.
- **Plus Five Five, Inc. (Resend)** — SCCs + EU-US DPF. Verarbeitet ausschließlich E-Mail-Adressen. TIA vorhanden: *Resend Vendor Security Assessment (2026-03-02)*.
- **Sentry, Inc.** — SCCs + EU-US DPF. PII-Scrubbing vor Übermittlung angewandt. TIA vorhanden: *Sentry Vendor Risk Assessment*.
- **Haufe-Lexware GmbH & Co. KG (Lexware)** — EU (Deutschland) ansässig; unmittelbar DSGVO und BDSG unterworfen. Kein grenzüberschreitender Übermittlungsmechanismus erforderlich. Verarbeitet Rechnungs- und Buchhaltungsdaten, die Kontaktname, E-Mail-Adresse, Postanschrift und Steueridentifikationsnummern des Kunden umfassen können. TIA vorhanden: *Lexware Vendor Security Assessment (2026-03-13)*.

Voice2Evolve verpflichtet sich außerdem, **Angemessenheitsbeschlüsse und Übermittlungsmechanismen regelmäßig zu überprüfen**, um die fortlaufende Einhaltung von Art. 46 DSGVO sicherzustellen. Kunden können Kopien oder Zusammenfassungen relevanter TIAs auf begründete Anfrage erhalten.

Übermittlungen außerhalb des EWR stützen sich auf:

- EU-Standardvertragsklauseln (Anlage C),
- UK-Addendum (Anlage D) oder
- Angemessenheitsbeschlüsse bzw. andere zulässige Garantien.

Voice2Evolve stellt sicher, dass in Drittstaaten übermittelte Daten auf einem der DSGVO gleichwertigen Niveau geschützt bleiben.

---

10. Compliance-Verifikation und Dokumentation

Voice2Evolve stellt die zum Nachweis der Compliance vernünftigerweise erforderlichen Informationen durch schriftliche Dokumentation und Remote-Assurance-Maßnahmen bereit, die Sicherheit, Vertraulichkeit und die Privatsphäre anderer Kunden schützen. Routinemäßige Vor-Ort-Inspektionen privater Wohnsitze, Homeoffices oder Rechenzentren Dritter werden nicht angeboten.

- Der Kunde kann jährlich oder nach einer bestätigten Verletzung des Schutzes personenbezogener Daten, die Kundendaten betrifft, Compliance-Informationen anfordern.
- Voice2Evolve kann solche Anfragen durch Richtlinien, Sicherheitszusammenfassungen, Antworten auf Fragebögen, Zusammenfassungen unabhängiger Auditberichte oder Zertifizierungen sowie Remote-Erläuterungstermine erfüllen.
- Jede Prüfung, die über Dokumentation oder Remote-Review hinausgeht, setzt die vorherige schriftliche Zustimmung von Voice2Evolve oder eine eindeutige zwingende gesetzliche Anforderung einer zuständigen Aufsichtsbehörde voraus.
- Alle zur Nachweisführung erforderlichen Unterlagen werden vorgehalten und auf Anfrage bereitgestellt, vorbehaltlich Vertraulichkeits-, Sicherheits- und Verhältnismäßigkeitsschutzmaßnahmen.

---

11. Haftung

Die Gesamthaftung jeder Partei aus oder im Zusammenhang mit diesem MDPA ist auf die in den zwölf (12) Monaten vor dem haftungsbegründenden Ereignis nach der Vereinbarung gezahlten Entgelte begrenzt.

Diese Begrenzung gilt nicht für: (a) Haftung aufgrund von Vorsatz oder Betrug; (b) Verstöße gegen anwendbare Datenschutzgesetze, soweit eine Begrenzung nach zwingendem Recht unzulässig ist;
(c) Verletzungen von Vertraulichkeitspflichten.

Jede Partei ist allein verantwortlich für Verwaltungsstrafen, Bußgelder oder Sanktionen, die durch eine Aufsichtsbehörde unmittelbar gegen sie wegen eigener Nicht-Compliance verhängt werden.

---

12. Koordination bei Beschwerden und Untersuchungen

Der Kunde informiert Voice2Evolve unverzüglich über Beschwerden, Anfragen oder Untersuchungen einer Aufsichtsbehörde oder betroffener Personen in Bezug auf Verarbeitungen nach diesem MDPA. Beide Parteien arbeiten vollständig zusammen und teilen relevante Informationen, um konsistente und rechtskonforme Antworten zu gewährleisten.

13. Schweizer Datenschutz (DSG) – Konformität

Voice2Evolve erfüllt auch die Anforderungen des **Schweizer Bundesgesetzes über den Datenschutz (DSG/FADP)**. Für Datenübermittlungen aus der Schweiz gelten die gleichen Garantien, Standardvertragsklauseln und Sicherheitsmaßnahmen wie in diesem MDPA beschrieben. Zuständige Aufsichtsbehörde ist der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB/FDPIC)**.

14. Anwendbares Recht und Gerichtsstand

Dieses MDPA unterliegt dem Recht der **Bundesrepublik Deutschland**. Gerichtsstand für alle Streitigkeiten ist **Stuttgart, Deutschland**, sofern zwingendes Recht nichts anderes vorsieht.

15. Datenaufbewahrung und Löschung

Voice2Evolve unterhält klare Aufbewahrungs- und Löschfristen, um Art. 30 und 32 DSGVO zu erfüllen. Personenbezogene Daten werden nur so lange gespeichert, wie es zur Erfüllung der Verarbeitungszwecke oder zur Einhaltung gesetzlicher Pflichten erforderlich ist. Aufbewahrungsfristen werden anhand folgender Kriterien festgelegt:

- **Sitzungs-Transkripte:** Die Aufbewahrungsdauer richtet sich nach der vom Kunden konfigurierbaren Einstellung (7–365 Tage; Standardwert: 30 Tage). Nach Ablauf der Frist kann der Kunde wählen, ob Transkripte an Stelle gelöscht oder anonymisiert werden – d. h. der Gesprächsinhalt wird durch einen Schwärzungsvermerk ersetzt, während Sitzungsmetadaten erhalten bleiben. Die Anonymisierung bei Fristablauf ist standardmäßig aktiviert. Sofern der Kunde keine Aufbewahrungseinstellung vorgenommen hat, werden Transkripte innerhalb von 30 Tagen nach Sitzungsabschluss anonymisiert oder gelöscht.
- **Sitzungsanalysen und -bewertungen (Nicht-Transkript-Daten):** Bewertungen, Analyseergebnisse, Verhaltensmetriken und sonstige nicht-transkriptbezogene Sitzungsdaten werden für die Dauer des Nutzerkontos gespeichert und innerhalb von 30 Tagen nach Kontoschließung gelöscht, sofern der Kunde oder die betroffene Person nicht früher eine Löschung beantragt.

- **Interne Qualitätsbewertungsberichte:** Berichte, die vom automatisierten internen Qualitätsbewertungssystem von Voice2Evolve erstellt werden, werden 30 Tage aufbewahrt und anschließend gelöscht. Diese Berichte bewerten ausschließlich die eigenen KI-Systemkomponenten von Voice2Evolve und enthalten keine nutzerbezogenen Bewertungsdaten. Siehe Abschnitt 16.1.
- **Anonymisierte Aggregatdaten:** Vollständig anonymisierte, k-anonyme Verhaltensaggregatdaten – aus denen keine Einzelperson, Sitzung oder Organisation re-identifiziert werden kann – werden auf unbestimmte Zeit aufbewahrt, da sie nicht in den Anwendungsbereich des Begriffs „personenbezogene Daten" im Sinne von Art. 4 Nr. 1 DSGVO und Erwägungsgrund 26 fallen. Siehe Abschnitt 16.2.
- **Datenrückgabe nach Vertragsende:** Nach Beendigung oder Ablauf der Vereinbarung stellt Voice2Evolve die personenbezogenen Daten des Kunden für einen Zeitraum von neunzig (90) Kalendertagen zum Export bereit. Nach Ablauf dieses Übergangszeitraums löscht oder anonymisiert Voice2Evolve alle verbleibenden personenbezogenen Daten gemäß diesem Abschnitt 15, sofern keine gesetzliche Aufbewahrungspflicht besteht.
- **Kontodaten:** Speicherung für die Dauer des Kontos; sichere Löschung innerhalb von 30 Tagen nach Schließung.
- **Zahlungs- und Abrechnungsunterlagen:** Aufbewahrung für gesetzliche steuer- und handelsrechtliche Fristen (typischerweise 6–10 Jahre) und anschließende Löschung.
- **Audit- und Sicherheitsprotokolle:** Aufbewahrung für 90 Tage, sofern nicht längere Speicherung für Vorfalluntersuchungen oder Compliance erforderlich ist.

Voice2Evolve stellt sicher, dass Löschungen mittels sicherer Verfahren erfolgen und Audit-Trails zur Dokumentation der Löschung geführt werden. Aufbewahrungsrichtlinien werden jährlich überprüft und bei Bedarf an regulatorische und betriebliche Änderungen angepasst.

---

16. Zulässige Eigenverarbeitungszwecke von Voice2Evolve

Unbeschadet von Abschnitt 4 Ziffer 1 sind die nachfolgenden Eigenverarbeitungszwecke von Voice2Evolve durch die Vereinbarung ausdrücklich gestattet und stellen keine Verarbeitung außerhalb der dokumentierten Weisungen des Kunden dar:

16.1 Interne Qualitätsbewertung

Voice2Evolve betreibt ein automatisiertes Qualitätsbewertungssystem, das Sitzungs-Transkripte und Analyseergebnisse mithilfe von Unterauftragsverarbeitern (KI-Sprachmodell-Dienste gemäß Anlage B) ausschließlich zur Bewertung der Leistung eigener KI-Systemkomponenten von

Voice2Evolve verarbeitet – darunter Gesprächsplaner, Echtzeit-Dialogagent, Orchestrator und Nachsitzungsanalysator. Diese Verarbeitung dient dem Zweck, die technische Qualität der gegenüber dem Kunden erbrachten Leistungen aufrechtzuerhalten und kontinuierlich zu verbessern. Sie bewertet keine einzelnen Nutzer, erzeugt keine nutzergerichteten Ausgaben und erstellt weder Nutzer-Scores noch Nutzerprofile. Qualitätsbewertungsberichte sind ausschließlich intern bei Voice2Evolve verfügbar, über die kundenseitige Anwendung nicht zugänglich und werden innerhalb von 30 Tagen gelöscht.

16.2 Anonymisierte Aggregatanalysen

Wie durch die Vereinbarung und diesen Abschnitt 16.2 gestattet, leitet Voice2Evolve aus Sitzungsdaten vollständig anonymisierte, aggregierte Verhaltensstatistiken ab, um die Dienste zu verbessern und Produkt-Benchmarks zu entwickeln. Vor der Aggregation werden alle direkten und indirekten Identifikatoren – einschließlich Mandanten-ID, Sitzungs-ID und Nutzer-ID – entfernt. Die Aggregation unterliegt k-Anonymitätsschwellenwerten (mindestens 50 Sitzungen je Dimensionsgruppe); Gruppen unterhalb dieses Schwellenwerts werden vollständig ausgeschlossen. Nach erfolgter Anonymisierung gemäß diesem Standard stellen die entstehenden Daten keine personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DSGVO und Erwägungsgrund 26 mehr dar und unterliegen nicht den Beschränkungen dieses MDPA.

ANLAGE A – SICHERHEITSMASSNAHMEN

(Detaillierte Ausführung gemäß Art. 32 DSGVO)

Technische Maßnahmen:

- **Verschlüsselung:** AES-256-Verschlüsselung bei Speicherung und TLS 1.3 bei Übertragung. Schlüsselverwaltung gemäß ISO 27001 und NIST SP 800-57 (Erzeugung, Rotation, Vernichtung).
- **Zugriffskontrolle:** Rollenbasierte Zugriffskontrolle (RBAC) mit Multifaktor-Authentifizierung (MFA). Vergabe nach dem Prinzip der geringsten Rechte, quartalsweise Reviews und Protokollierung.
- **Logging und Monitoring:** Zentrale Protokollierung administrativer und systemischer Zugriffe; manipulationssichere Logs, Aufbewahrung mindestens 90 Tage, Anomalie-Prüfungen.
- **Netzwerksicherheit:** Voice2Evolve betreibt ausschließlich verwaltete Platform-as-a-Service-(PaaS-)Infrastruktur. Netzwerkschutzmaßnahmen – einschließlich DDoS-Abwehr, Firewall-Regeln, Traffic-Isolation und Intrusion-Detection – werden von den jeweiligen Infrastrukturanbietern bereitgestellt und betrieben (siehe Anlage B). Der administrative Zugriff auf

Anbieterplattformen ist durch Multifaktor-Authentifizierung gesichert und auf autorisiertes Personal beschränkt.
- **Pseudonymisierung:** Pseudonymisierung von Analyse- und Transkriptionsdaten durch Trennung von Identifikatoren und Zufalls-Tokens.
- **Sichere Softwareentwicklung:** Security-Maßnahmen im SDLC (Code-Reviews, Dependency-Checks, Vulnerability-Scanning vor Deployments).
- **Backup und Wiederherstellung:** Tägliche verschlüsselte Backups in EU-Rechenzentren, 30-Tage-Aufbewahrung, quartalsweise Wiederherstellungstests.

Organisatorische Maßnahmen:

- **Security-Governance:** Jährliche Überprüfung der Informationssicherheitsrichtlinien durch das Management.
- **Vertraulichkeit:** Vertraulichkeits- und Datenschutzvereinbarungen für Mitarbeitende und Auftragnehmer.
- **Schulung:** Jährliche Datenschutz- und Sicherheitsschulungen für alle Mitarbeitenden mit Zugriff auf personenbezogene Daten.
- **Vendor-Management:** Risiko-Assessment und DPA-Prüfung für Unterauftragsverarbeiter vor Einsatz. Unterauftragsverarbeiter werden vertraglich verpflichtet, Datenschutzschulungen für Personal durchzuführen, das personenbezogene Daten verarbeitet.
- **Incident Response:** Dokumentierte Verfahren zur Erkennung, Eskalation, Eindämmung und Nachbereitung; Meldungen ohne unangemessene Verzögerung nach Art. 33 DSGVO.
- **Audit und Review:** Halbjährliche interne Audits; unabhängige Berichte/Zertifizierungen, sofern verfügbar.
- **Business Continuity:** Getestete Pläne für Disaster-Recovery, Redundanz und Notfallmaßnahmen.
- **Physische Sicherheit:** Voice2Evolve betreibt keine eigenen Rechenzentren. Die gesamte Infrastruktur wird von Drittanbietern gehostet, deren Einrichtungen branchenübliche physische Sicherheitskontrollen einhalten, einschließlich ISO-27001- oder SOC-2-Zertifizierung, Zugangskontrollen und Umgebungsüberwachung. Anbieterzertifizierungen werden im Rahmen des oben beschriebenen Vendor-Management-Prozesses überprüft.

ANLAGE B – UNTERAUFTRAGSVERARBEITER

Voice2Evolve unterhält einen dokumentierten Prozess zur regelmäßigen Überprüfung und Aktualisierung von Unterauftragsverarbeitern und erteilt Kunden eine allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern gemäß Art. 28 Abs. 2 DSGVO. Kunden können

Änderungsbenachrichtigungen abonnieren, um eine angemessene Vorankündigung über neue Unterauftragsverarbeiter zu erhalten.

Anbieter	Rolle	Standort	Rechtsgrundlage / Garantien
Supabase Inc.	Datenbank, Authentifizierung	EU (Stockholm, Schweden als primäres Hosting); Weiterübermittlungen an Unterauftragsverarbeiter in USA / Singapur	Supabase DPA + SCCs + ergänzende Schutzmaßnahmen gemäß Supabase-TIA
OpenAI, L.L.C.	KI-Inference / Voice API	USA	SCCs + CPRA-Compliance
Stripe Payments Europe Ltd.	Zahlungen	EU / USA	GDPR DPA + SCCs
Vercel Inc.	Frontend-Hosting	EU / USA	SCCs
Railway.app	Backend-Infrastruktur	EU	GDPR DPA
Cloudflare, Inc.	DNS-Auflösung, WebRTC-TURN-Relay	EU / USA	GDPR DPA + SCCs
Sentry, Inc.	Fehler-Monitoring	EU / USA	GDPR DPA + SCCs
Rybbit	Website- und Produktanalyse (nur ausgewählte App-Seiten; sensible Pfade ausgeschlossen)	EU (EWR — Hetzner)	GDPR DPA + SCCs
Plus Five Five, Inc. (Resend)	Transaktionale E-Mails	USA	GDPR DPA + SCCs + EU-US DPF
Anthropic PBC	KI-Inference (LLM)	USA	GDPR DPA + SCCs
Haufe-Lexware GmbH & Co. KG (Lexware)	Rechnungs- und Buchhaltungssynchronisation	EU (Deutschland)	GDPR DPA (AVV)

ANLAGE C – STANDARDVERTRAGSKLAUSELN (VOLLSTÄNDIGER TEXT)

Hinweis: Anlage C wird im englischen Originaltext wiedergegeben, da die Standardvertragsklauseln durch Verweis auf den amtlichen Wortlaut in die Vereinbarung einbezogen werden und Übersetzungen hiervon abweichen können. Maßgeblich bleibt der amtliche Text im Amtsblatt der Europäischen Union.

Pursuant to GDPR Article 46 and EU Commission Implementing Decision (EU) 2021/914, the Standard Contractual Clauses (Module 2: Controller to Processor)

are hereby incorporated by reference in their entirety and form an integral part of this Agreement. The official full text is published in the *Official Journal of the European Union* (OJ L 199, 7.6.2021, p. 31–61) and is available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

The key provisions of the EU Standard Contractual Clauses are summarized below for convenience. In the event of any discrepancy between this summary and the official text, the official text shall prevail.

SECTION I – PURPOSE AND SCOPE

(Clauses 1–7 summarized from EU Commission Implementing Decision (EU) 2021/914)

Clause 1 – Purpose and Scope The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 for the transfer of personal data to a third country.

Clause 2 – Effect and Invariability of the Clauses These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies.

Clause 3 – Third-Party Beneficiaries Data subjects may enforce these Clauses as third-party beneficiaries.

Clause 4 – Interpretation Terms used shall have the meaning given in the GDPR.

Clause 5 – Hierarchy In the event of a contradiction, these Clauses shall prevail.

Clause 6 – Description of the Transfer(s) The details of the transfer(s) are specified in Annex I.

Clause 7 – Docking Clause An entity not party to these Clauses may accede to them at any time with agreement of the Parties.

SECTION II – OBLIGATIONS OF THE PARTIES

(Clauses 8–10 summarized)

Clause 8 – Data Protection Safeguards The data importer shall process the personal data only on documented instructions from the data exporter.

Clause 9 – Use of Subprocessors The data importer has the data exporter’s general authorization for the engagement of subprocessors as detailed in Annex III.

Clause 10 – Data Subject Rights The data importer shall assist the data exporter in fulfilling data subject rights under GDPR Articles 15–22.

SECTION III – LOCAL LAWS AND ACCESS BY AUTHORITIES

(Clauses 14–15 summarized)

Clause 14 – Local Laws and Practices The Parties warrant that they have no reason to believe the laws of the third country prevent the importer from fulfilling these Clauses.

Clause 15 – Obligations of the Data Importer in Case of Access by Public Authorities The data importer agrees to notify the data exporter of any legally binding request for disclosure by a public authority.

SECTION IV – FINAL PROVISIONS

(Clauses 16–18 summarized)

Clause 16 – Non-Compliance and Termination If the importer is in breach of these Clauses, the exporter may suspend the transfer or terminate the contract.

Clause 17 – Governing Law These Clauses are governed by the laws of Germany, allowing for third-party beneficiary rights.

Clause 18 – Choice of Forum and Jurisdiction Any dispute shall be resolved by the courts of Germany. Data subjects may also bring legal proceedings before their habitual residence courts within the EU.

ANNEX I – DETAILS OF THE TRANSFER

A. List of Parties

- **Data Exporter (Controller):** The Customer as identified in the Agreement.
- **Data Importer (Processor):** Voice2Evolve UG (haftungsbeschränkt), registered in Germany. Contact: privacy@voice2evolve.com.

B. Description of Transfer

- **Categories of Data Subjects:** End users (employees, candidates, or other individuals) who use the Services on behalf of or at the direction of the Customer.
- **Categories of Personal Data:** Voice recordings, session transcripts, session analytics and scores, user account data (name, email address), usage metadata, and IP addresses.
- **Special Categories of Data:** None (see Section 2.5).

- **Frequency of Transfer:** Continuous, for the duration of the Agreement.
- **Nature and Purpose of Processing:** Bereitstellung KI-basierter Sprach-Sparring-, Trainings-, Transkriptions-, Bewertungs- und Analyseleistungen gemäß der Vereinbarung und Abschnitt 2.3.
- **Retention Period:** As specified in Section 15.

C. Competent Supervisory Authority The competent supervisory authority is the data protection authority of the EU Member State in which the Data Exporter is established, or — where the Data Exporter is not established in the EU — the supervisory authority of the Member State in which the Data Exporter's EU representative is established. Where neither applies, the competent authority is the Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (Germany).

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES See Attachment A (Security Measures)

ANNEX III – SUBPROCESSORS See Attachment B (Subprocessors)

The official text of EU Commission Implementing Decision (EU) 2021/914 (Controller → Processor, Module 2) is incorporated by reference and executed by both Parties. Annex I–III are populated as follows:

- Annex I: See above (Details of the Transfer).
- Annex II: Security Measures (Attachment A).
- Annex III: Subprocessors (Attachment B).

ANLAGE D – UK-ADDENDUM (ICO)

Gilt für Datenübermittlungen aus dem Vereinigten Königreich nach dem vom ICO genehmigten Addendum zu den EU-SCCs. Das Addendum stellt rechtmäßige Übermittlungen nach UK GDPR und Data Protection Act 2018 sicher.

Kernbestimmungen:

- Die EU-Standardvertragsklauseln (Modul 2) werden mit den nach dem UK-Addendum erforderlichen Änderungen übernommen.
- Verweise auf die DSGVO gelten als Verweise auf die UK GDPR.
- Verweise auf die Europäische Union oder Mitgliedstaaten schließen das Vereinigte Königreich ein.
- Zuständige Aufsichtsbehörde ist das **Information Commissioner’s Office (ICO)**.
- Anwendbares Recht und Gerichtsstand: **England und Wales**.

Diese Bestimmungen stellen rechtmäßige Datenübermittlungen zwischen dem Vereinigten Königreich und Drittstaaten nach UK-Datenschutzrecht sicher.

ANLAGE D.1 – SCHWEIZ-ADDENDUM (DSG/FADP)

Gilt für Datenübermittlungen aus der Schweiz gemäß dem **Schweizer Bundesgesetz über den Datenschutz (DSG/FADP)** und der zugehörigen Verordnung. Für Übermittlungen aus der Schweiz werden die gleichen EU-Standardvertragsklauseln (Modul 2) mit erforderlichen Anpassungen übernommen:

- Verweise auf die DSGVO sind als Verweise auf das DSG/FADP zu verstehen.
- Zuständige Aufsichtsbehörde ist der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB/FDPIC)**.
- Verweise auf EU-Mitgliedstaaten umfassen die Schweiz.

Diese Klauseln stellen sicher, dass Datenübermittlungen aus der Schweiz in Drittstaaten ein angemessenes Schutzniveau gewährleisten, das dem nach DSG/FADP erforderlichen Niveau entspricht.

ANLAGE E – US-DATENSCHUTZ-ADDENDUM

Diese Anlage gilt nur, soweit und in dem Umfang, in dem anwendbare US-Datenschutzgesetze der Bundesstaaten die Nutzung der Leistungen durch den Kunden regeln.

Voice2Evolve handelt als **Service Provider** und **Processor** nach anwendbaren US-Bundesstaaten-Datenschutzgesetzen, einschließlich, aber nicht beschränkt auf:

- **California Consumer Privacy Act (CCPA)** in der durch den **California Privacy Rights Act (CPRA)** geänderten Fassung,
- **Virginia Consumer Data Protection Act (CDPA)**,
- **Colorado Privacy Act (CPA)**,
- **Connecticut Data Privacy Act (CTDPA)**,
- und jedes andere US-Bundesstaaten-Datenschutzgesetz, das Voice2Evolve im Zusammenhang mit den Leistungen Pflichten als Auftragsverarbeiter oder Service Provider auferlegt.

Nach diesen Gesetzen wird Voice2Evolve:

1. personenbezogene Daten ausschließlich auf dokumentierte Weisungen des Kunden und zu vertraglichen Geschäftszwecken verarbeiten,

2. personenbezogene Daten weder verkaufen noch teilen noch für zielgerichtete Werbung, Profiling oder nicht vertraglich vereinbarte Zwecke verwenden,
3. den Kunden (Verantwortlichen) bei der Beantwortung verifizierter Verbraucherrechte-Anträge unterstützen (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Opt-out von zielgerichteter Werbung),
4. sicherstellen, dass Weiterübermittlungen personenbezogener Daten den anwendbaren staatlichen Anforderungen und vertraglichen Garantien entsprechen,
5. angemessene Sicherheitspraktiken entsprechend der Sensibilität der personenbezogenen Daten umsetzen,
6. Dokumentation von Verarbeitungstätigkeiten und Datenschutz-Assessments führen, soweit gesetzlich erforderlich,
7. den Kunden unverzüglich über Datenschutzverletzungen, Beschwerden oder Anfragen in Bezug auf CDPA/CPRA informieren,
8. dem Kunden eine Compliance-Prüfung durch Dokumentation und Remote-Assurance-Maßnahmen gemäß Abschnitt 10 ermöglichen,
9. personenbezogene Daten auf Anfrage oder bei Beendigung der Vereinbarung löschen oder zurückgeben, sofern keine gesetzliche Aufbewahrungspflicht besteht.

Die Datenaufbewahrung bleibt auf die Leistungsdauer oder gesetzliche Pflichten beschränkt. Voice2Evolve bestätigt die Einhaltung aller anwendbaren US-Bundesstaaten-Datenschutzregelungen für seine Rolle als Auftragsverarbeiter/Service Provider.

Dieses MDPA wird elektronisch geschlossen und ist integraler Bestandteil der Vereinbarung. Es wird rechtsverbindlich mit der elektronischen Annahme der Vereinbarung durch den Kunden, einschließlich per Checkbox oder vergleichbarem Mechanismus.

Company address: Grabenstr. 26, 71254 Ditzingen, Germany

VAT ID: DE459808424