Auftragsverarbeitungsvertrag (AVV)

Vertrag nach Art. 28 DSGVO zwischen dem Restaurant und Voizely. Wird BEVOR der erste echte Anruf live geht unterzeichnet — kein "wir holen das später nach."

Parteien

Auftraggeber (Verantwortlicher):

`[Restaurant-Firmierung]`

`[Anschrift]`

`[Vertretungsberechtigter Name + Funktion]`

— im Folgenden "Restaurant" —

Auftragnehmer (Auftragsverarbeiter):

NPC Agency / Voizely

Inhaber: Ilia Isachev

Fürth / Nürnberg, Bayern, Deutschland

info@npc-agency.com · +49 176 3051 3266

— im Folgenden "Voizely" —

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Voizely erbringt für das Restaurant einen AI-gestützten Telefonempfang für eingehende Reservierungs-Anrufe sowie ein Self-Service-Onboarding für die Einrichtung des Dienstes. Im Rahmen dieser Leistungen verarbeitet Voizely personenbezogene Daten von Gästen und vom verantwortlichen Restaurant-Personal im Auftrag des Restaurants.

(2) Die Verarbeitung dauert für die Laufzeit des zugrundeliegenden Hauptvertrags (Voizely-Angebot, separat). Mindestlaufzeit drei (3) Monate.

§ 2 Art und Zweck der Verarbeitung

(1) **Art der Verarbeitung:**

a) Laufzeitbetrieb des KI-Empfangs: Annahme von Telefonanrufen, Spracherkennung (Sprache → Text), Slot-Extraktion (Personenzahl, Datum, Uhrzeit, Name, optional Sonderwünsche), Verfügbarkeitsprüfung und Reservierungs-Schreibvorgang in das Buchungssystem des Restaurants.

b) Onboarding (Phase 5): Erfassung der Restaurant-Stammdaten über das Self-Service-Formular oder den Done-For-You-Admin-Modus; einmaliges Scrapen der Restaurant-Webseite zur Vorausfüllung von zwölf Sachfakten (Konzept, Öffnungszeiten, Speise-Stichworte); Zahlungsabwicklung (Setup-Fee + monatliche Subscription); Generierung und Provisionierung des KI-Assistenten.

(2) **Zweck:** Entlastung des Restaurant-Personals von telefonischen Reservierungsanfragen in Stoßzeiten und außerhalb der Geschäftszeiten; sowie Bereitstellung einer rechtssicheren, schnellen Einrichtung des Dienstes.

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) **Verarbeitete Daten — Anrufer-Daten (Gäste):**

• Name des Gastes • Telefonnummer (falls vom Gast genannt oder per Caller-ID übertragen) • Anzahl Personen • Datum und Uhrzeit der gewünschten Reservierung • Sonderwünsche (Free-Text, strukturiert pro Reservierung — z. B. *"Tisch am Fenster"*) • Sprachaufnahme (Transkript): Audio-Stream wird NICHT gespeichert; aus der Sprache abgeleitete Text-Transkripte werden 30 Tage gespeichert (siehe § 7).

(2) **Verarbeitete Daten — Restaurant-Verantwortliche (Phase 5 Onboarding):**

• Vor- und Nachname des Vertretungsberechtigten • Geschäfts-E-Mail-Adresse • Geschäfts-Telefonnummer für Rückrufe • Restaurant-Firmierung und -Anschrift • Umsatzsteuer-ID (falls vorhanden) • Zahlungsdaten **(verarbeitet durch Stripe — Voizely sieht NUR die letzten vier Stellen der Karte oder die IBAN; keine PAN, keine CVV)** • IP-Adresse und User-Agent bei AVV-Annahme (Art. 28 Audit-Trail).

(3) **Anrufaufnahme ist standardmäßig DEAKTIVIERT.** Optional kann das Restaurant Aufnahme für QA aktivieren; dies erfordert eine Anpassung des Hauptvertrags und eine zusätzliche Hinweistafel am Telefon-Begrüßungsskript ("Dieser Anruf wird aufgezeichnet").

(4) **Betroffene Personen:** Gäste des Restaurants, die anrufen; sowie die vertretungsberechtigte Person des Restaurants beim Onboarding.

§ 4 Pflichten des Auftragnehmers

Voizely:

(1) Verarbeitet Daten ausschließlich auf dokumentierte Weisung des Restaurants.

(2) Stellt sicher, dass zur Verarbeitung befugte Personen sich zur Vertraulichkeit verpflichtet haben.

(3) Trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM):

• Verschlüsselung aller API-Zugangsdaten im Ruhezustand (pgsodium / Supabase Vault). • Zugriff auf die Datenbank nur über Service-Role-Key serverseitig; Mandantenisolation per Row-Level Security. • Verbindung zu allen Unterauftragsverarbeitern verschlüsselt (TLS 1.2+). • Anrufaufnahme standardmäßig deaktiviert. • 30-Tage-Löschkonzept für Transkripte als pg_cron-Job *voizely_purge_old_transcripts*. • Content-Security-Policy mit per-Request-Nonce auf allen Seiten des Onboarding-Formulars. • Brute-Force-Schutz auf dem Magic-Link-Login (Tabelle *login_attempts*, 5 Versuche / 15 Minuten je IP). • Pro-IP-Rate-Limit auf dem Formular gegen Bot-Spray; zusätzlich Cloudflare Turnstile. • **AVV-Audit-Trail nach BEG IV 2025 Textform:** bei Klick auf die AVV-Checkbox werden vier Belegspuren in *onboarding_intakes* geschrieben — *avv_accepted_at*, *avv_ip*, *avv_user_agent*, *avv_pdf_version* (Version dieses Dokuments). • Strukturierte Erfassung von Allergie-Hinweisen am Reservierungsobjekt — KEINE Speicherung gesundheitsbezogener Aussagen im Free-Text-Transkript über die 30-Tage-Frist hinaus.

(4) Unterstützt das Restaurant bei der Beantwortung von Anträgen Betroffener (Art. 15–22 DSGVO).

(5) Meldet Datenschutzverletzungen unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, an das Restaurant.

§ 5 Unterauftragsverarbeiter

(1) Das Restaurant erteilt Voizely die allgemeine Genehmigung, die folgenden Unterauftragsverarbeiter einzusetzen. Stand bei Vertragsschluss (**Stand: 2026-05-25 — v1**):

1	Twilio Inc.	Telefonie — DE-Inbound-Nummer, Voice-Routing	USA (DE-PoP für Anrufe)	SCCs + Twilio DPA + EU-US DPF wo einschlägig
2	Vapi Inc.	Voice-Orchestrierung (STT↔LLM↔TTS-Pipeline, Tool-Call-Dispatch)	USA (managed)	SCCs + Vapi DPA — v1 ersetzt Vapi durch Pipecat
3	Gladia SAS	Spracherkennung Deutsch (Solaria-1 Modell)	EU (Frankreich) — ISO 27001	Direkter AVV (EU-EU)
4	Mistral AI	LLM (Dialog-Logik, Slot-Extraktion, Tool-Call-Entscheidungen)	EU (Frankreich)	Direkter AVV (EU-EU)
5	ElevenLabs Inc.	**Primäre** TTS (Sprachsynthese, Stimme "Benjamin")	USA	SCCs (Modul 2) + ElevenLabs DPA + per-Restaurant-AVV-Addendum
5b	Microsoft Azure Speech	**Fallback**-TTS (Stimme de-DE-FlorianMultilingualNeural)	EU Data Boundary (westeurope / germanywestcentral)	Microsoft Online Services DPA + EU Data Boundary
6	Supabase Inc.	Datenbank — System of Record für alle Restaurant-, Anruf- und Onboarding-Daten	EU (Frankfurt, eu-central-1)	Direkter AVV + Supabase Vault / pgsodium für Credentials
7	Stripe Payments Europe Ltd.	Zahlungsabwicklung (Setup-Fee + monatliche Subscription); Rechnungsadresse + Tax-ID	EU (Irland) — IBAN-Lastschrift via SEPA	Stripe Data Processing Agreement
8	Resend, Inc.	Transaktionale E-Mails (Welcome, Resume-Link, Voice-Clone-Bestätigung)	USA	SCCs (Modul 2) + Resend DPA
9	OpenAI, L.L.C.	Webseiten-Faktenextraktion (gpt-4o-mini, Structured Outputs — 12 Tier-1-Fakten)	USA	SCCs + OpenAI DPA — kein Training auf Kundendaten (API-default)
10	Firecrawl	Webseiten-Scraping als Vorstufe der Faktenextraktion	USA	SCCs + Firecrawl Terms; **Fallback**: Server-side cheerio (EU, keine Datenausleitung)
11	Cloudflare, Inc. (Turnstile)	Bot-Schutz auf dem Onboarding-Formular (Captcha-Ersatz)	USA / globales CDN	Cloudflare DPA — Token-only, kein Inhalt der Form-Daten

(2) Voizely informiert das Restaurant über beabsichtigte Änderungen der Sub-Prozessor-Liste mit einer Frist von mindestens 30 Tagen. Das Restaurant kann der Änderung schriftlich widersprechen.

(3) Voizely stellt sicher, dass jeder Unterauftragsverarbeiter mindestens die gleichen Datenschutzpflichten einhält wie sie in diesem AVV vereinbart sind. Soweit erforderlich (US-Empfänger ohne Angemessenheitsbeschluss) werden Standardvertragsklauseln der Europäischen Kommission abgeschlossen.

§ 6 Drittlandtransfer

(1) Verarbeitungen in Drittländern (insbesondere USA bei Twilio, Vapi, ElevenLabs, Resend, OpenAI, Firecrawl und Cloudflare) erfolgen auf Grundlage von Standardvertragsklauseln der Europäischen Kommission (Art. 46 DSGVO) sowie — soweit einschlägig — des EU-US Data Privacy Framework.

(2) **Voizely verzichtet ausdrücklich auf die Aussage "Alle Daten bleiben in der EU"** für den v0-Zeitraum, da Vapi und ElevenLabs US-gehostet sind. Diese Aussage wird in einem zukünftigen Release (v1, Pipecat-Migration) freigeschaltet.

§ 7 Löschung und Rückgabe

(1) **Transkripte werden 30 Tage nach Erstellung automatisch gelöscht.** Implementiert als Postgres-pg_cron-Job *voizely_purge_old_transcripts*.

(2) Reservierungs-Daten verbleiben im Buchungssystem-Konto des Restaurants. Voizely löscht sein eigenes operationelles Logbuch bei Beendigung des Hauptvertrags auf Weisung des Restaurants.

(3) Aufzeichnungen werden — falls aktiviert — nicht gespeichert, da im v0-Standard deaktiviert.

(4) Abgebrochene Onboarding-Intakes (Status *pending*) werden nach 30 Tagen automatisch gelöscht (TTL-Cronjob *expire-onboarding-intakes*).

§ 8 Kontroll- und Auskunftsrechte

Das Restaurant ist berechtigt, sich von der Einhaltung dieses Vertrags durch Voizely zu überzeugen. Voizely erteilt auf Anfrage Auskunft über die TOM, den Datenfluss und die Sub-Prozessoren.

Ort, Datum

_____

Restaurant

_____
Unterschrift & Stempel

Voizely / NPC Agency

_____
Ilia Isachev, Inhaber