AUFTRAGSVERARBEITUNGSVERTRAG

HOSTSYSTEM . GEMÄSS ART. 28 DSGVO

AUFTRAGNEHMER / AUFTRAGSVERARBEITER

HostSystem ist ein System von **CK GrowthSystems**
(eine Marke der CK Global GbR)
Kirchstraße 22C, 77736 Zell am Harmersbach
hello@ckgrowthsystems.com
USt-IdNr.: DE357817554

(im Folgenden „Auftragnehmer" oder „Auftragsverarbeiter")

AUFTRAGGEBER / VERANTWORTLICHER

UNTERNEHMEN
_____

ADRESSE
_____

E-MAIL
_____

ANSPRECHPARTNER
_____

(im Folgenden „Auftraggeber" oder „Verantwortlicher")

*– gemeinsam auch **„Vertragsparteien"** genannt –*

§ 1 Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Mit diesem Vertrag wird sichergestellt, dass die Anforderungen der Datenschutz-Grundverordnung bei der Übermittlung personenbezogener Daten an einen Auftragnehmer eingehalten werden. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist dafür verantwortlich, zu beurteilen, ob die Datenverarbeitungsvorgänge nach Art. 6 DSGVO zulässig sind, und die Betroffenenrechte zu wahren.

1.2 Dieser Vertrag gilt für die Übermittlung personenbezogener Daten gemäß **Anlage 1**. Die Anlagen zu diesem Vertrag sind ebenfalls Bestandteil dieses Vertrages.

1.3 Dieser Vertrag enthält alle wichtigen Garantien und durchsetzbaren Rechte für die betroffenen Personen sowie wirksame Rechtsbehelfe gemäß Art. 46 Abs. 1 und Art. 46 Abs. 2 lit. c DSGVO.

1.4 Dieser Vertrag gilt unabhängig von den übrigen Verpflichtungen des Auftraggebers gemäß der DSGVO.

1.5 Der genaue Gegenstand der Datenübermittlung, die betroffenen Datenkategorien sowie der Verarbeitungszweck sind in Anlage 1 beschrieben.

1.6 Der Auftraggeber versichert, sich im Rahmen des Möglichen davon überzeugt zu haben, dass der Auftragnehmer durch geeignete technische und organisatorische Maßnahmen in der Lage ist, seinen Pflichten aus diesem Vertrag nachzukommen.

1.7 Die Daten werden vorrangig in Deutschland, einem EU-Land oder einem Land des Europäischen Wirtschaftsraums verarbeitet. Eine Verarbeitung in Drittländern erfolgt nur unter den Voraussetzungen von Kapitel 5 DSGVO (Art. 44 ff.) und unter Einhaltung der EU-Standardvertragsklauseln (SCC). Die genutzten Drittland-Auftragsverarbeiter sind in **Anlage 3** aufgeführt; mit Vertragsschluss willigt der Auftraggeber in deren Beauftragung ein.

1.8 Die Vergütung wird außerhalb dieses Vertrags in einem **gesonderten Dienstleistungsvertrag** zwischen den Parteien vereinbart. Diese AVV ist von der Vergütung unabhängig.

§ 2 Vertragslaufzeit und Kündigung

Dieser Auftragsverarbeitungsvertrag gilt für die Dauer der Leistungsbeziehung zwischen den Parteien auf Basis des jeweiligen Dienstleistungsvertrages und der HostSystem-AGB. Er endet automatisch mit Beendigung der Leistungsbeziehung.

§ 3 Weisungen des Auftraggebers

3.1 Der Auftraggeber ist berechtigt, dem Auftragnehmer Weisungen zur Verarbeitung personenbezogener Daten zu erteilen, insbesondere zur Löschung, Berichtigung, Sperrung oder Herausgabe. Der Auftragnehmer hat diese Weisungen zu befolgen, sofern sie nicht gegen geltendes Recht verstoßen.

3.2 Hält der Auftragnehmer eine Weisung für rechtswidrig, hat er den Auftraggeber unverzüglich zu informieren und kann die Ausführung bis zur Bestätigung oder Änderung durch den Auftraggeber vorübergehend aussetzen.

3.3 Weisungen sind schriftlich oder in elektronischer Form (z. B. per E-Mail) zu erteilen. Mündliche Weisungen sind vom Auftragnehmer zu protokollieren (Datum, Uhrzeit, beteiligte Personen).

3.4 Der Auftraggeber kann weisungsberechtigte Personen benennen. Änderungen sind unverzüglich mitzuteilen.

§ 4 Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, im erforderlichen Umfang die Einhaltung der datenschutz- und datensicherheitsrechtlichen Vorschriften beim Auftragnehmer zu kontrollieren, auch durch beauftragte Dritte. Der Auftragnehmer hat diese Kontrollen zu dulden und zu unterstützen sowie alle erforderlichen Informationen vollständig und wahrheitsgemäß zur Verfügung zu stellen.

4.2 Da HostSystem als Cloud-Plattform betrieben wird, erfolgen Kontrollen in der Regel über die Auswertung von TOM-Dokumentationen, Audit-Berichten der Sub-Auftragsverarbeiter (z. B. SOC 2, ISO 27001 von Supabase, Hostinger) sowie schriftlichen Auskünften. Vor-Ort-Kontrollen erfolgen zu den üblichen Geschäftszeiten nach angemessener Voranmeldung, sofern der Kontrollzweck keine vorherige Ankündigung ausschließt.

4.3 Ergebnisse von Kontrollen und erteilte Weisungen sind von beiden Parteien zu protokollieren.

§ 5 Allgemeine Pflichten des Auftragnehmers

5.1 Die Daten werden ausschließlich auf Grundlage dieses Vertrages und der Weisungen des Auftraggebers verarbeitet. Eine anderweitige Verarbeitung ist nur bei zwingenden gesetzlichen Verpflichtungen zulässig; der Auftraggeber ist vorab zu informieren, sofern keine gesetzliche Mitteilungspflicht entgegensteht.

5.2 Der Auftragnehmer hat bei der Auftragsdurchführung alle einschlägigen gesetzlichen Vorschriften einzuhalten, insbesondere die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO umzusetzen sowie das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO zu führen.

5.3 Sofern der Auftragnehmer zur Benennung eines Datenschutzbeauftragten verpflichtet ist, hat er dessen Kontaktdaten dem Auftraggeber mitzuteilen. Änderungen sind unverzüglich bekanntzugeben.

5.4 Datenverarbeitung außerhalb der Betriebsstätten des Auftragnehmers (z. B. Homeoffice, Fernzugriff) erfolgt im Rahmen der vereinbarten technischen und organisatorischen Maßnahmen (verschlüsselte Verbindungen, MFA, getrennte Geräte).

5.5 Der Auftragnehmer hat sicherzustellen, dass alle mit der Verarbeitung befassten Personen einer Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor Unterzeichnung der Verschwiegenheitsverpflichtung darf kein Zugang zu den personenbezogenen Daten erfolgen.

5.6 Auf Anfrage stellt der Auftraggeber der betroffenen Person eine Kopie dieses Vertrages einschließlich der Anlagen unentgeltlich zur Verfügung. Vertrauliche Informationen und Geschäftsgeheimnisse können vor der Weitergabe unkenntlich gemacht werden; eine aussagekräftige Zusammenfassung ist beizufügen.

5.7 Der Auftragnehmer kontrolliert die Erfüllung seiner Pflichten regelmäßig und eigenständig und dokumentiert dies in geeigneter Weise.

§ 6 Sensible Daten

Soweit die Verarbeitung besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO umfasst — insbesondere **Gesundheitsdaten** (z. B. Allergie-Hinweise, Unverträglichkeiten, Hinweise auf Schwangerschaft) oder **Daten über religiöse Überzeugungen** (z. B. religiös motivierte Speise-Vorgaben), die der Gast freiwillig im Rahmen einer Reservierung mitteilen kann — wendet der Auftragnehmer die in **Anlage 2** beschriebenen speziellen Beschränkungen und zusätzlichen Schutzmaßnahmen an.

§ 7 Technische und organisatorische Maßnahmen

7.1 Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Die mindestens umzusetzenden Maßnahmen sind in **Anlage 2** aufgeführt. Der Auftragnehmer überprüft diese regelmäßig auf Angemessenheit.

7.2 Der Auftragnehmer beschränkt den Datenzugang auf Personen, die diesen für die Vertragserfüllung benötigen, und stellt deren Verschwiegenheitsverpflichtung sicher.

7.3 Bei Verletzungen des Schutzes personenbezogener Daten hat der Auftragnehmer unverzüglich Abhilfemaßnahmen zu ergreifen, die Folgen zu minimieren und den Auftraggeber **innerhalb von 24 Stunden nach Kenntniserlangung** zu informieren. Die Meldung enthält: Kontaktdaten der Anlaufstelle, Beschreibung der Verletzung, betroffene Datenkategorien und -mengen, wahrscheinliche Folgen sowie ergriffene und geplante Maßnahmen.

7.4 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der DSGVO-Vorgaben, einschließlich der Benachrichtigung der zuständigen Aufsichtsbehörde und betroffener Personen.

§ 8 Unterstützungspflichten des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrung der Betroffenenrechte gemäß Kapitel III DSGVO (Art. 12–22), insbesondere bei Auskunft, Löschung, Berichtigung und Einschränkung der Verarbeitung. Hierzu stellt HostSystem dem Auftraggeber im UI direkt nutzbare Werkzeuge zur Verfügung (Datenexport, Anonymisierungsfunktion im Bereich „Datenschutz / DSGVO“).

8.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten gemäß Art. 32–36 DSGVO (Datensicherheit, Meldepflichten, Datenschutz-Folgenabschätzung).

§ 9 Einsatz von Unterauftragnehmern (Subunternehmer)

9.1 Der Auftragnehmer nimmt weitere Auftragnehmer (Unterauftragnehmer) nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Auftraggebers in Anspruch (Art. 28 Abs. 2 S. 1 DSGVO). Die Regelungen gelten für alle nachgelagerten Unterauftragnehmer.

9.2 Mit Unterzeichnung dieses Vertrages erteilt der Auftraggeber seine Zustimmung zur Beauftragung der in **Anlage 3** aufgeführten Unterauftragnehmer, vorbehaltlich einer vertraglichen Vereinbarung gemäß Art. 28 Abs. 2 und 4 DSGVO.

9.3 Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Hinzuziehungen oder Wechsel von Unterauftragnehmern. Der Auftraggeber kann innerhalb von **14 Tagen** aus wichtigem Grund schriftlich widersprechen. Nach Ablauf dieser Frist gilt die Genehmigung als erteilt.

9.4 Bei Unterauftragnehmern in Drittstaaten sind die besonderen Voraussetzungen der Art. 44 ff. DSGVO einzuhalten. Der Auftragnehmer schließt mit diesen Unterauftragnehmern EU-Standardvertragsklauseln (SCC) ab und prüft ergänzende Maßnahmen (Transfer Impact Assessment).

9.5 Der Auftragnehmer gewährleistet, dass dem Auftraggeber gegenüber dem Unterauftragnehmer dieselben Anordnungs- und Kontrollrechte zustehen wie ihm gegenüber dem Auftragnehmer. Bei Pflichtverletzungen durch einen Unterauftragnehmer haftet der Auftragnehmer gegenüber dem Auftraggeber.

9.6 Auf Anfrage erhält der Auftraggeber eine Kopie der Untervergabevereinbarung; vertrauliche Informationen können geschwärzt werden.

§ 10 Mitteilungspflichten des Auftragnehmers

10.1 Bei Verstößen gegen diesen Vertrag, die Weisungen des Auftraggebers oder gegen datenschutzrechtliche Bestimmungen — auch bei begründetem Verdacht — ist der Auftraggeber unverzüglich zu informieren. Diese Pflicht gilt für den Auftragnehmer sowie alle eingesetzten Personen und Unterauftragnehmer.

10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Informationspflichten nach Art. 33 und 34 DSGVO. Meldungen an Behörden oder Betroffene dürfen erst nach vorheriger Weisung des Auftraggebers erfolgen.

10.3 Anfragen von Betroffenen, Behörden oder Dritten (Auskunft, Berichtigung, Sperrung, Löschung) leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter. Eine eigenständige Bearbeitung erfolgt nur auf Weisung des Auftraggebers.

10.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich über behördliche Maßnahmen sowie über Ereignisse, die die vertragsgegenständlichen Daten gefährden könnten.

§ 11 Vertragsbeendigung, Löschung und Rückgabe der Daten

11.1 Nach Abschluss der Verarbeitung oder bei Vertragsende hat der Auftragnehmer alle personenbezogenen Daten zu löschen oder zurückzugeben, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

11.2 Der Auftraggeber hat **30 Tage** nach Vertragsende Zeit, seine Daten über die in HostSystem integrierten Export-Funktionen herunterzuladen (CSV, JSON — DSGVO Art. 20).

11.3 Nach Ablauf dieser 30-Tage-Frist werden alle Tenant-Daten endgültig gelöscht; eine Wiederherstellung ist dann nicht mehr möglich. Backups werden im Rahmen der ohnehin gültigen Backup-Rotationen ebenfalls überschrieben (max. 7 Tage nach Tenant-Löschung).

11.4 Der Auftraggeber ist berechtigt, die Löschmaßnahmen zu überprüfen und Löschprotokolle anzufordern.

§ 12 Datengeheimnis und Vertraulichkeit

12.1 Der Auftragnehmer ist unbefristet — auch nach Vertragsende — verpflichtet, personenbezogene Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln zu beachten (z. B. § 203 StGB). Der Auftraggeber hat den Auftragnehmer bei Auftragserteilung auf besondere Geheimnisschutzregeln hinzuweisen.

12.2 Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung befassten Mitarbeiter die Datenschutzbestimmungen und Geheimnisschutzregeln kennen und einhalten, insbesondere bei Aufnahme ihrer Tätigkeit.

12.3 Der Auftragnehmer dokumentiert die Einhaltung dieser Ziffer und stellt die Dokumentation dem Auftraggeber auf Anfrage zur Verfügung.

§ 13 Haftung

13.1 Jede Partei haftet der anderen gegenüber für Schäden, die durch Verstöße gegen diesen Vertrag verursacht werden.

13.2 Verstößt der Auftragnehmer oder ein Unterauftragnehmer gegen diesen Vertrag, kann die betroffene Person Schadensersatz für materielle und immaterielle Schäden verlangen.

13.3 Der Auftragnehmer haftet gegenüber betroffenen Personen für jeden Schaden, der durch eine Verletzung ihrer Rechte als Drittbegünstigte entsteht (Art. 82 DSGVO), unabhängig davon, ob der Schaden durch den Auftraggeber oder den Auftragnehmer verursacht wurde.

13.4 Bei gesamtschuldnerischer Haftung mehrerer Parteien gegenüber der betroffenen Person ist ein interner Ausgleich entsprechend dem jeweiligen Verschuldensanteil vorzunehmen.

13.5 Der Auftragnehmer kann sich nicht durch Verweis auf Fehler eines Unterauftragnehmers entlasten; er haftet für die ordnungsgemäße Leistungserbringung aller eingesetzten Subunternehmer.

§ 14 Schlussbestimmungen

14.1 Änderungen und Ergänzungen dieses Vertrages sowie Nebenabreden bedürfen der Schriftform oder elektronischen Form; der Änderungsgegenstand muss eindeutig bezeichnet sein.

14.2 Verweise auf DSGVO-Vorschriften gelten entsprechend für Nachfolgeregelungen, soweit diese inhaltlich übereinstimmen.

14.3 Die Unwirksamkeit einzelner Bestimmungen lässt die Wirksamkeit der übrigen Bestimmungen unberührt. Unwirksame Bestimmungen sind durch wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommen.

14.4 Sämtliche Anlagen sind Bestandteil dieses Vertrages.

UNTERSCHRIFTEN

AUFTRAGNEHMER (AN) · CK GROWTHSYSTEMS / HOSTSYSTEM

_____

Ort, Datum

_____

Unterschrift

AUFTRAGGEBER (AG)

_____

Ort, Datum

_____

Unterschrift

Anlage 1 — Auftragsdetails

Der vorliegende Vertrag umfasst (im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

- Bereitstellung und Betrieb der **HostSystem-SaaS-Plattform** (Multi-Tenant-Reservierungs- und Tischverwaltung)
- Einrichtung, Konfiguration und Betrieb von **Voice-AI-Telefonagenten** (über die Demandly-Plattform, technisch realisiert über GoHighLevel)
- Versand transaktionaler **E-Mail-Bestätigungen** an Restaurant-Gäste (über Resend)
- Versand von **WhatsApp-Bestätigungen** an Restaurant-Gäste (über Demandly/GoHighLevel oder Meta Cloud API, je nach Tenant-Konfiguration)
- Verarbeitung und Speicherung von **Reservierungsdaten** und zugehörigen Kommunikationsverläufen
- Bereitstellung von **Statistik- und Analyse-Funktionen** (Auslastung, Reservierungs-Volumen, Voice-Call-Outcome)
- **DSGVO-Compliance-Werkzeuge** (Datenexport, Anonymisierungsfunktion, Löschung)
- Protokollierung, Administration, Fehleranalyse und Systemsicherheit

ART DER VERARBEITUNG

Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Verwenden, Übermitteln, Bereitstellen, Abgleichen, Einschränken, Löschen und gegebenenfalls Anonymisieren personenbezogener Daten im Rahmen der Leistungserbringung.

ZWECK DER VERARBEITUNG

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zum Zweck der Bereitstellung, Durchführung und technischen Unterstützung der vertraglich geschuldeten Leistungen des Auftragsverarbeiters, insbesondere:

- Annahme von Tischreservierungen über automatisierte Sprach- und Chat-Agenten
- Versand von Bestätigungen, Stornos und Erinnerungen an die hinterlegten Kontaktdaten der Gäste
- Bereitstellung der Reservierungs-Übersicht für das Restaurant-Team
- Bereitstellung von Voice-AI-Anrufprotokollen zur Qualitätssicherung
- Erfüllung gesetzlicher Pflichten (Buchführung, Steuern)

VERARBEITETE DATENKATEGORIEN

- **Stammdaten** (Vorname, Nachname, ggf. „Familie“-/Höflichkeitsangaben)
- **Kontaktdaten** der Gäste (Telefonnummer, E-Mail-Adresse — je nach gewähltem Bestätigungs-Kanal)
- **Reservierungsdaten** (Datum, Uhrzeit, Personenzahl, Tisch-/Bereichszuweisung, Buchungsnummer, Status)
- **Kommunikationsdaten** (Voice-Call-Transkripte, WhatsApp-Nachrichteninhalte, E-Mail-Inhalte, Notizen)
- **Sprachaufzeichnungen** (Voice-Call-Audio, sofern Demandly/GoHighLevel diese speichert)
- **Sondermerkmale** auf Wunsch des Gasts (z. B. Allergie-Hinweise, Kinderstuhl-Bedarf, Rollstuhl-Zugänglichkeit, religiöse Speise-Vorgaben — siehe § 6)
- **Technische Daten** (IP-Adresse, Geräte- und Browserinformationen, Logfiles, Zeitstempel)
- **Authentifizierungsdaten** des Restaurant-Teams (E-Mail, gehashtes Passwort, Session-Tokens)
- **Metadaten der Kommunikation** (Anrufzeitpunkt, Anrufdauer, Outcome, ggf. Anrufer-ID)

KREIS DER BETROFFENEN PERSONEN

- **Gäste** des Auftraggebers, die Reservierungen über die Voice-AI, WhatsApp, E-Mail oder durch das Restaurant-Team manuell anlegen lassen
- **Anrufer** der Voice-AI, auch wenn keine Reservierung zustande kommt
- **Mitarbeiter** des Auftraggebers (Restaurant-Inhaber, Manager, Service-Personal), die das HostSystem nutzen
- **Sonstige Personen**, die über die Plattform-Kanäle (Voice, Chat, E-Mail) mit dem Auftraggeber in Kontakt treten

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt.

I. Zweckbindung und Trennbarkeit (Mandantenfähigkeit)

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken bzw. von unterschiedlichen Tenants erhobene Daten getrennt verarbeitet werden:

- **Multi-Tenant-Architektur** mit logischer Mandantentrennung über *restaurant_id* als Pflichtfeld in jeder Datentabelle
- **Postgres Row-Level Security (RLS)** mit Policies pro Tabelle, die jeden Datensatz auf den eigenen Tenant beschränken
- **Berechtigungskonzept** mit drei Rollen pro Tenant (Owner, Manager, Staff)
- **Trennung von Produktiv- und Test-System** (separate Datenbanken)
- **Verschlüsselte Datenübertragung** (TLS 1.2+, HTTPS-only)
- Versehen aller Datensätze mit Tenant-Attribut, automatischer Zugriffsfilter über Supabase-RLS

II. Vertraulichkeit und Integrität

1. Verschlüsselung

Die Übertragung personenbezogener Daten erfolgt ausschließlich über verschlüsselte Verbindungen (TLS 1.2+, HTTPS). Gespeicherte Daten werden durch Verschlüsselungsmechanismen der eingesetzten Cloud-Infrastruktur geschützt (Encryption at Rest — Supabase/PostgreSQL mit AES-256). Passwörter werden mittels bcrypt/argon2 (Supabase Auth) gehasht und gesalzen. API-Tokens (z. B. Meta WhatsApp Access Tokens) werden in der Datenbank verschlüsselt gespeichert und in API-Antworten redacted.

2. Pseudonymisierung

- Die im Rahmen der Plattform verarbeiteten personenbezogenen Daten werden grundsätzlich nicht pseudonymisiert, da die direkte Kommunikation mit Gästen dies erfordert (Reservierungsbestätigung mit Namen). Bei Vertragsende erfolgt jedoch automatisch eine Anonymisierung gemäß § 11 dieses Vertrages.

3. Zutrittskontrolle (Maßnahmen gegen unbefugten Zutritt)

Da HostSystem als Cloud-Plattform betrieben wird, erfolgt die physische Zutrittskontrolle durch die eingesetzten Cloud- und Hosting-Anbieter:

- Physische Zutrittskontrollen der Rechenzentren (Hostinger, Supabase) inkl. Zugangskontrollen, Sicherheitszonen, Videoüberwachung
- Schließsysteme, Alarmanlagen, 24/7-Sicherheitspersonal in den Rechenzentren
- Zertifizierungen der Cloud-Anbieter (ISO 27001, SOC 2)
- Eigene Mitarbeiter des Auftragnehmers haben keinen physischen Zugang zur Hosting-Infrastruktur

4. Zugangskontrolle (Maßnahmen gegen unbefugte Systemnutzung)

- Zuordnung von **Benutzerrechten** über Supabase Auth + Memberships-Tabelle
- **Benutzerprofile** mit Rolle (Owner / Manager / Staff)
- **Passwort-Richtlinien** (Mindestlänge, Komplexität gemäß Supabase-Auth-Standard)

- **Authentifikation** mit Benutzername/Passwort, optional 2FA für Owner-Rolle
- **Session-Tokens** mit angemessener Lebensdauer, JWT-basiert
- **Rate-Limiting** auf Login-Endpoint und API zur Abwehr von Brute-Force
- **Verschlüsselung mobiler IT-Systeme** der Mitarbeiter des Auftragnehmers (FileVault, BitLocker)
- **Hardware- und Software-Firewalls** auf Mitarbeiter-Geräten
- **Anti-Viren-Software** auf allen Endgeräten
- **VPN-Technologie** für administrative Zugriffe
- **Sperren externer Schnittstellen** (USB-Restriktionen auf Admin-Geräten)

5. Zugriffskontrolle

- **Berechtigungskonzept** mit drei Rollen pro Tenant
- **Verwaltung der Rechte** durch Tenant-Owner; Wechsel über Supabase + Memberships-API
- **Regelmäßige Überprüfung** der Zugriffsrechte
- **Anzahl der Administratoren** auf notwendiges Minimum reduziert (CK GrowthSystems-Mitarbeiter mit Service-Role-Key in Supabase)
- **Passwortrichtlinie** inkl. Mindestlänge und Komplexität
- **Rollenbasierte Zugriffskontrolle** in Datenbank-Policies (RLS)
- **Service-Role-Key** wird ausschließlich serverseitig verwendet, nie an Client ausgeliefert
- **Sub-Auftragsverarbeiter-Zugriff** vertraglich gebunden gemäß Art. 28 DSGVO

6. Eingabekontrolle

- **Protokollierung** der Eingabe, Änderung und Löschung von Daten in der *voice_events*-Tabelle (Voice-AI-bezogen) und über Supabase Audit-Logs
- **Nachvollziehbarkeit** durch individuelle Benutzer-IDs (UUID pro Mitarbeiter)
- **Vergabe von Rechten** zur Eingabe, Änderung und Löschung auf Basis des Berechtigungskonzepts
- **Systemprotokolle und Logfiles** zur Nachverfolgung von Systemzugriffen und Änderungen
- **Sentry Error-Logging** mit personenbezogene-Daten-Filter

7. Auftragskontrolle

- **Auswahl der Sub-Auftragsverarbeiter** unter Sorgfaltsgesichtspunkten (DSGVO-Konformität, Zertifizierungen, Standort)
- **Vorherige Prüfung** und Dokumentation der Sicherheitsmaßnahmen
- **Schriftliche Auftragsverarbeitungsverträge** (DPA / AVV) mit allen Sub-Verarbeitern
- **Verpflichtung der Mitarbeiter** auf das Datengeheimnis
- **Sicherstellung der Löschung** von Daten nach Beendigung des Auftrags
- **Kontrollrechte** gegenüber den Sub-Auftragsverarbeitern vereinbart
- **Laufende Überprüfung** der Sub-Auftragsverarbeiter und ihrer Tätigkeiten
- Einsatz ausschließlich vertraglich gebundener Unterauftragsverarbeiter gemäß Art. 28 DSGVO

8. Weitergabekontrolle

- **TLS-/HTTPS-Verschlüsselung** der Kommunikationswege
- **API-Authentifizierung** über Webhook-Secrets pro Tenant (für Voice-AI-Endpoints)
- **Verschlüsselte Datenübertragung** zwischen Plattform, APIs und eingesetzten Cloud- und Kommunikationsdiensten
- **Idempotency-Keys** zur Verhinderung doppelter Datenverarbeitung bei Netzwerk-Retries
- **Rate-Limiting** zur Abwehr von Daten-Exfiltrations-Versuchen

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit

- **Hochverfügbare Cloud-Infrastruktur** mit redundanten Systemen und Monitoring (Hostinger, Supabase)
- **Unterbrechungsfreie Stromversorgung** und Klimatisierung in den Rechenzentren der Cloud-Anbieter
- **Feuer- und Rauchmeldeanlagen** in den Rechenzentren der Cloud-Anbieter
- **Backup-Konzept**: Tägliche Backups mit Point-in-Time-Recovery für die letzten 7 Tage (über Supabase)
- **Belastbares Wiederherstellungskonzept** vorhanden — Restore innerhalb weniger Stunden möglich
- **Notfallplan** für längere Ausfälle (manuelle Reservierungsannahme über Telefon-Fallback während Wiederherstellung)
- **Health-Check-Endpoint** (*/api/health*) für externe Uptime-Überwachung
- **Sentry Error-Tracking** zur frühen Fehler-Erkennung
- **Monitoring** der API-Performance und der Sub-Auftragsverarbeiter-Verfügbarkeit

IV. Besondere Datenschutzmaßnahmen

- **Interne Verhaltensregeln** für den Umgang mit personenbezogenen Daten
- **Datensicherheitskonzept** auf Basis der hier dokumentierten TOMs
- **Wiederanlaufkonzept** auf Basis der Backup-Strategie (siehe III)
- **Risikoanalyse** im Rahmen der Verarbeitungsverzeichnis-Pflege
- **Daten-Minimierungs-Prinzip** bei der Verarbeitung — es werden nur die für die Reservierungsabwicklung erforderlichen Daten erhoben
- **Automatische PII-Anonymisierung** alter Voice-Calls (>90 Tage) durch nächtlichen Cleanup-Job
- **Webhook-Log-TTL** (>30 Tage werden gelöscht)
- **Idempotency-Log-TTL** (>24 Stunden werden gelöscht)
- **Regelmäßige Überprüfung** der technischen und organisatorischen Maßnahmen

V. Überprüfung der Maßnahmen

Der Auftragnehmer prüft, evaluiert und passt die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von **12 Monaten** sowie anlassbezogen an. Wesentliche Änderungen werden dem Auftraggeber mitgeteilt.

Anlage 3 — Genehmigte Unterauftragnehmer (Subunternehmer)

Mit Unterzeichnung dieses Vertrages erteilt der Auftraggeber seine Zustimmung zur Beauftragung folgender Unterauftragnehmer:

UNTERNEHMEN	LEISTUNG	ORT	KONTAKT
Hostinger International Ltd.	Hosting der Plattform-Infrastruktur (Application + statischer Content)	EU (Litauen)	hostinger.com
Supabase Inc.	Datenbank, Authentifizierung, Realtime-Updates, Backups	USA / EU-Region (Frankfurt)	supabase.com
Resend Inc.	Versand transaktionaler E-Mails (Bestätigungen, Reminder, Daily Digest)	USA / EU-Region	resend.com
HighLevel LLC (Demandly)	Voice-AI, WhatsApp-Versand, Workflow-Automatisierung	USA	gohighlevel.com
Meta Platforms Ireland Ltd.	WhatsApp Business Cloud API (optional pro Tenant)	Irland	meta.com
Functional Software, Inc. (Sentry)	Fehler-Logging und Performance-Monitoring (optional)	USA	sentry.io
Vercel Inc.	Hosting der Plattform-Infrastruktur (Application, Edge-Functions, Static Content) sowie Web-Analytics (Page-Views, cookieless, nur nach Consent gemäß Cookie-Banner)	USA / EU-Region	vercel.com

Alle eingesetzten Unterauftragnehmer wurden vertraglich gemäß Art. 28 DSGVO verpflichtet. Bei Sub-Auftragsverarbeitern in Drittstaaten (USA) basiert der Datentransfer auf den **EU-Standardvertragsklauseln (SCC)** gemäß Durchführungsbeschluss (EU) 2021/914 sowie ergänzenden Maßnahmen (Verschlüsselung, Zugriffskontrollen).

Bei Hinzuziehung oder Wechsel von Unterauftragnehmern wird der Auftraggeber gemäß § 9.3 dieses Vertrages informiert.

Dieser AVV wurde mit rechtlicher Sorgfalt erstellt und ersetzt keine individuelle Rechtsberatung. Vor produktivem Einsatz wird eine Prüfung durch eine spezialisierte Anwaltskanzlei (IT-Recht / Datenschutz) empfohlen.