AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO

VERTRAGSPARTEIEN

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):
KugelAudio UG (haftungsbeschränkt)
Schäfertrift 6
30657 Hannover
Deutschland
Vertreten durch: Geschäftsführer Kajo Kratzenstein

Handelsregister: Amtsgericht Hannover, HRB 277989 B

---

§ 1 GELTUNGSBEREICH

(1) Dieser Vertrag regelt die Auftragsverarbeitung von personenbezogenen Daten gemäß Art. 28 DSGVO zwischen dem Auftraggeber (im Folgenden „Kunde") und dem Auftragnehmer KugelAudio UG (im Folgenden „KugelAudio").

(2) Dieser Vertrag ist integraler Bestandteil der Servicevereinbarung / Nutzungsbedingungen zwischen den Parteien (im Folgenden „Hauptvertrag").

---

§ 2 GEGENSTAND UND DAUER DER AUFTRAGSVERARBEITUNG

(1) **Gegenstand:** KugelAudio stellt eine KI-gestützte Sprachverarbeitungsplattform (Speech-to-Speech / Text-to-Speech) über API- und Web-Interfaces sowie das Hosting der dafür notwendigen Infrastruktur bereit. Alle Verarbeitungen erfolgen ausschließlich auf Weisung des Auftraggebers und gemäß der im Hauptvertrag definierten Servicelogik.

(2) **Dauer:** Die Verarbeitung beginnt mit Inkrafttreten dieses Vertrags und wird für die Dauer der Leistungserbringung durchgeführt. Im Falle einer Beendigung des Hauptvertrags endet dieses Auftragsverarbeitungsverhältnis spätestens 30 Tage nach Kündigungsmitteilung. Bestimmungen zur Datenlöschung gelten unabhängig davon.

---

§ 3 ART, ZWECK UND UMFANG DER VERARBEITUNG

(1) **Verarbeitungsvorgänge:** KugelAudio führt folgende Verarbeitungsvorgänge durch:

- Erheben und Auslesen von Audio-Daten (Sprachaufnahmen)
- Verarbeitung von Textdaten (Input-Prompts, Transkripte)
- Synthetisierung und Konvertierung mittels KI-Modellen (TTS/STT)
- Speicherung von Stimm-Referenzen (Voice Cloning Samples), sofern vom Kunden bereitgestellt
- Kurzzeitige, temporäre Speicherung im RAM während Verarbeitung
- Streaming von Audio-Output an die Endnutzer des Kunden
- Erstellung von technischen Logs und Nutzungsmetadaten

(2) **Zweck:**

- Ermöglichung von Echtzeit-Sprachinteraktionen für Endanwendungen des Auftraggebers
- Erbringung der Voice-AI-Services gemäß Hauptvertrag
- Training und Inferenz von KI-Stimmmodellen (sofern separat beauftragt)
- Technisches Monitoring, Support und Abrechnung

(3) **Art der Daten:**

- **Audiodaten:** Sprachaufnahmen von Endnutzern des Kunden
- **Textdaten:** Input-Prompts, Transkripte, Konfigurationsparameter
- **Metadaten:** Zeitstempel, User-IDs, Organisation-IDs, Model-IDs, API-Key-IDs, Request-Größen, Processing-Zeiten
- **Voice References:** Optional hochgeladene Stimm-Samples für Voice Cloning
- **Technische Logs:** Error-Logs, Request-Logs (keine Inhalts-Payloads)

(4) **Betroffene Personen:**

- Kunden und Nutzer des Auftraggebers
- Mitarbeiter des Auftraggebers (soweit diese mit KugelAudio-Services interagieren)

(5) **Kategorien von Empfängern:** Siehe § 6 (Unterauftragsverarbeiter) und Anlage 2.

---

§ 4 PFLICHTEN DES AUFTRAGGEBER

(1) Der Auftraggeber verpflichtet sich, KugelAudio nur entsprechend diesen Vertragsbedingungen und anwendbaren Datenschutzgesetzen zu beauftragen.

(2) Der Auftraggeber trägt die volle Verantwortung dafür, dass die an KugelAudio übermittelten Daten rechtmäßig erhoben wurden und die Verarbeitung rechtlich zulässig ist (Basis: Einwilligung, Vertrag, gesetzliche Verpflichtung o. ä.).

(3) Der Auftraggeber versichert, dass ihm alle erforderlichen Einwilligungen der betroffenen Personen vorliegen oder dass die Verarbeitung auf sonstige Rechtsgründe gestützt werden kann.

---

§ 5 PFLICHTEN DES AUFTRAGSVERARBEITERS (KUGELAUDIO)

(1) **Verarbeitung nach Weisung:** KugelAudio verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und gemäß den im Hauptvertrag beschriebenen Funktionalitäten. Zusätzliche Verarbeitungen erfolgen nur nach vorheriger schriftlicher Genehmigung.

(2) **Vertraulichkeit:** KugelAudio verpflichtet sich, dass nur autorisierte Personen Zugang zu den Daten des Auftraggebers haben. Alle Mitarbeiter und Subunternehmer werden schriftlich zur Vertraulichkeit verpflichtet.

(3) **Sicherheitsmaßnahmen:** KugelAudio implementiert und erhält die in Anlage 1 aufgeführten technischen und organisatorischen Maßnahmen (TOMs) ein. Im Falle von Sicherheitslücken benachrichtigt KugelAudio den Auftraggeber unverzüglich.

(4) **Trennung der Daten:** Im Rahmen dieses Auftrags verarbeitete Daten werden von sonstigen Datenbeständen logisch und technisch getrennt.

(5) **Keine Vervielfältigungen ohne Wissen des Auftraggebers:** Kopien oder Duplikate werden nicht erstellt, ausgenommen:

- Technisch notwendige, temporäre Vervielfältigungen im RAM während der Verarbeitung
- Datensicherungen gemäß § 5(7)

(6) **Datensicherungen:** KugelAudio führt regelmäßige, verschlüsselte Backups der Stamm- und Konfigurationsdaten durch und dokumentiert diese. Backups werden gemäß den geltenden Aufbewahrungsfristen aufbewahrt.

(7) **Nachweis der Compliance:** KugelAudio erbringt auf Anforderung des Auftraggebers den Nachweis der Erfüllung seiner Sicherheitspflichten, insbesondere:

- Dokumentation der technischen und organisatorischen Maßnahmen
- Nachweise müssen spätestens auf Anforderung innerhalb von 30 Arbeitstagen vorgelegt werden

(8) **Regelmäßige Überprüfung:** KugelAudio überprüft die Wirksamkeit der Sicherheitsmaßnahmen mindestens jährlich.

---

§ 6 UNTERAUFTRAGSVERARBEITER (SUBUNTERNEHMER)

(1) **Allgemeine Genehmigung:** Der Auftraggeber erteilt KugelAudio die generelle Genehmigung, weitere Auftragsverarbeiter (Subunternehmer / Sub-Processor) hinzuzuziehen. Die derzeit eingesetzten Subunternehmer sind in **Anlage 2** aufgeführt.

(2) **Benachrichtigungspflicht:** KugelAudio informiert den Auftraggeber vor der Hinzuziehung oder des Austauschs eines Subunternehmers (via E-Mail oder Dashboard-Notifikation mit angemessener Vorausfrist).

(3) **Widerspruchsrecht:** Der Auftraggeber kann gegen die Hinzuziehung oder den Austausch eines Subunternehmers innerhalb von 4 Wochen nach Zugang der Benachrichtigung schriftlich Widerspruch einlegen. Der Widerspruch muss aus einem wichtigen datenschutzrechtlichen Grund erfolgen und begründet werden. Erfolgt kein fristgerechter oder begründeter Widerspruch, gilt die Änderung als genehmigt.

(4) **Vertragsgarantien:** Jeder Subunternehmer wird vertraglich darauf verpflichtet, mindestens die gleichen Datenschutzstandards einzuhalten wie in diesem Vertrag vereinbart. KugelAudio räumt dem Auftraggeber auf Anforderung Einsicht in die relevanten Vertragsbedingungen ein.

(5) **Verantwortlichkeit:** KugelAudio bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten durch Subunternehmer vollständig verantwortlich.

(6) **Weitere Unteraufträge (Kettengewährleistung)**:
Der Auftragnehmer verpflichtet seine direkten Unterauftragnehmer vertraglich dazu, die datenschutzrechtlichen Bestimmungen dieses Vertrags (insbesondere die Vorgaben aus Art. 28 Abs. 4 DSGVO) auch an deren eigene Unterauftragnehmer weiterzugeben. Eine gesonderte Genehmigung durch den Auftraggeber für die Hinzuziehung weiterer Unterauftragnehmer durch die Unterauftragnehmer (Sub-Sub-Unternehmer) ist nicht erforderlich, sofern das Datenschutzniveau gewahrt bleibt.

---

§ 7 BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN

(1) **Umsetzung von Anweisungen:** KugelAudio führt alle Anweisungen des Auftraggebers zur Berichtigung, Löschung oder Sperrung von Daten unverzüglich durch. Weisungen, die über die vertraglich vereinbarte Leistung oder Funktionalität hinausgehen oder technische Änderungen an der Plattform erfordern, bedürfen einer gesonderten Vereinbarung über die Kostentragung und Umsetzbarkeit.

(2) **Zeitrahmen:** Anweisungen werden innerhalb von 5 Arbeitstagen nach Eingang durchgeführt, sofern keine längere Frist technisch erforderlich oder gesetzlich vorgesehen ist.

(3) **Nachweis:** KugelAudio dokumentiert und bestätigt dem Auftraggeber die durchgeführten Maßnahmen.

(4) **Datenlöschung nach Vertragsende:** Nach Beendigung der Auftragsverarbeitung oder auf Wunsch des Auftraggebers werden alle im Auftrag verarbeiteten Daten gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht. Ausgenommen sind anonymisierte oder verschlüsselte Archivkopien, die für historische oder gesetzliche Compliance-Anforderungen notwendig sind.

---

§ 8 DATENSICHERHEITSVORFÄLLE (INCIDENTS)

(1) **Meldepflicht:** KugelAudio teilt dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten (Data Breach) unverzüglich, spätestens innerhalb von 72 Stunden nach Entdeckung mit.

(2) **Inhalt der Meldung:** Die Mitteilung enthält:

- Beschreibung des Sicherheitsvorfalls
- Betroffene Daten und betroffene Personen (soweit bekannt)
- Wahrscheinliche Folgen
- Ergriffene und geplante Abhilfemaßnahmen
- Kontaktperson bei KugelAudio für weitere Informationen

(3) **Unterstützung bei Notifizierung:** KugelAudio unterstützt den Auftraggeber bei der Erfüllung seiner Benachrichtigungspflichten gegenüber Aufsichtsbehörden (gem. Art. 33 DSGVO) und betroffenen Personen (gem. Art. 34 DSGVO).

(4) **Dokumentation:** Alle Vorfälle werden dokumentiert.

---

§ 9 BETROFFENENRECHTE

(1) **Unterstützung bei Auskunftsanfragen:** Auf Weisung des Auftraggebers kooperiert KugelAudio bei der Erfüllung von Auskunftsanfragen, Löschungsanfragen, Berichtigungsanfragen und sonstigen Rechten betroffener Personen gemäß Art. 15-22 DSGVO.

(2) **Informationspflicht:** KugelAudio stellt alle erforderlichen Informationen zur Verfügung, damit der Auftraggeber seinen Pflichten gemäß Art. 12-14 DSGVO (Benachrichtigung betroffener Personen) nachkommen kann.

(3) **Rückkehranforderung bei RighttoDataPortability:** Falls der Auftraggeber die Portabilität von Daten verlangt, stellt KugelAudio diese in einem strukturierten, gängigen, maschinenlesbaren Format bereit.

---

§ 10 KONTROLLRECHTE DES AUFTRAGGEBERS

(1) **Nachweise der Sicherheit:** KugelAudio weist die Einhaltung der technischen und organisatorischen Maßnahmen primär durch die Bereitstellung von aktuellen Eigenerklärungen, Dokumentationen der Sicherheitskonzepte oder Berichten über interne Sicherheitsüberprüfungen nach. Sofern KugelAudio zukünftig über externe Zertifizierungen (z. B. SOC 2, ISO 27001) verfügt, können diese Berichte die oben genannten Nachweise ersetzen oder ergänzen.

(2) **Inspektionen vor Ort:** Eine Überprüfung vor Ort ist nur zulässig, wenn der Auftraggeber nachweist, dass die in Abs. 1 genannten Nachweise (Dokumentationen, Berichte) nicht ausreichen, um die Einhaltung der Pflichten zu belegen, oder wenn zwingende gesetzliche Vorgaben dies erfordern. Solche Inspektionen sind mit einer Frist von mindestens vier (4) Wochen schriftlich anzukündigen und dürfen den Betriebsablauf nicht stören.

(3) **Kosten:** Der Auftraggeber trägt sämtliche Kosten der Inspektion (einschließlich der Kosten für externe Prüfer). Zusätzlich ist KugelAudio berechtigt, den eigenen Personalaufwand für die Begleitung der Inspektion zu angemessenen, marktüblichen Stundensätzen in Rechnung zu stellen, es sei denn, die Prüfung deckt erhebliche, vorsätzliche oder grob fahrlässige Verstöße von KugelAudio auf.

(4) **Subunternehmer:** KugelAudio gewährt Einsicht in die datenschutzrelevanten Teile der Verträge mit Unterauftragnehmern. Kommerzielle Konditionen oder Geschäftsgeheimnisse dürfen geschwärzt werden.

---

§ 11 DATENSCHUTZ-FOLGENABSCHÄTZUNG (DPIA)

(1) KugelAudio unterstützt den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung (DPIA) gemäß Art. 35 DSGVO, falls eine hochrisiko-Verarbeitung vorliegt.

(2) KugelAudio stellt erforderliche Informationen über seine technischen und organisatorischen Maßnahmen zur Verfügung.

---

§ 12 DATENSCHUTZBEAUFTRAGTER

Falls erforderlich, benennt KugelAudio einen Datenschutzbeauftragten und gibt dem Auftraggeber dessen Kontaktdaten bekannt.

---

§ 13 INTERNATIONALE DATENÜBERTRAGUNGEN

(1) **EU/EWR-Verarbeitung (Standard):** Die meisten Verarbeitungsvorgänge (Audio/Text-Daten) erfolgen ausschließlich auf Servern in der EU/EWR (Deutschland, Finnland).

(2) **USA-Dienstleister (Business-Daten):** Einige Subunternehmer (Vercel, Sentry) sind in den USA ansässig und verarbeiten dort ggf. Business-Daten (Account-Info, Abrechnungsdaten, nicht aber Audio/Text-Inhalte). Diese Übermittlungen erfolgen auf Grundlage:

- **EU-U.S. Data Privacy Framework** (falls der Anbieter zertifiziert ist), oder
- **EU-Standardvertragsklauseln (SCC)** als Transfermechanismus gem. Art. 46 DSGVO

(3) **Sicherheitsgewährleistung:** KugelAudio informiert den Auftraggeber über alle Länderübermittlungen und die angewendeten Schutzmaßnahmen.

---

§ 14 KOSTENZURECHENBARKEIT UND VERTRAGSLAUFZEIT

(1) **Kosten:** Die Kosten für die Auftragsverarbeitung sind in den Gebühren des Hauptvertrags enthalten. Zusätzliche Audits oder Compliance-Maßnahmen können gesondert berechnet werden.

(2) **Kündigung:** Dieser Vertrag läuft parallel zum Hauptvertrag. Im Falle einer Beendigung des Hauptvertrags endet auch dieses Auftragsverarbeitungsverhältnis.

---

§ 15 SCHLUSSBESTIMMUNGEN

(1) **Geltungsdauer:** Dieser Vertrag wird mit Abschluss des Hauptvertrags wirksam und läuft für die gesamte Dauer der Geschäftsbeziehung.

(2) **Änderungen:** Änderungen dieses Vertrags bedürfen der Schriftform (E-Mail genügt) und müssen von beiden Parteien unterzeichnet werden.

(3) **Salvatorische Klausel:** Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt der übrige Vertrag gültig. Die Parteien werden eine zulässige Regelung mit vergleichbarem Regelungszweck treffen.

(4) **Anwendbares Recht:** Dieser Vertrag unterliegt deutschem Recht. Gerichtsstand ist Hannover.

(5) **Datenschutzgesetze:** Die Einhaltung von DSGVO, BDSG und weiteren anwendbaren Datenschutzgesetzen ist verpflichtend.

ANLAGEN

ANLAGE 1: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

1. VERTRAULICHKEIT (ZUTRITTS-, ZUGANGS- UND ZUGRIFFSKONTROLLE)

1.1 Transportverschlüsselung

- **HTTPS/TLS:** Alle Web-Requests werden über TLS 1.2 oder höher verschlüsselt.
- **WSS (WebSocket Secure):** Echtzeit-Audio-Streaming läuft über verschlüsselte WebSocket-Verbindungen (wss://).
- **Zertifikate:** Let's Encrypt oder gleichwertige vertrauenswürdige Zertifizierungsstellen. Automatische Erneuerung.
- **SSL-Redirect:** HTTP-Requests werden automatisch auf HTTPS umgeleitet.

1.2 Authentifizierung & API-Sicherheit

- **API-Keys:** Zugriff auf API-Endpunkte erfolgt nur mit validierten API-Keys. Keys werden gekürzt bei der Anzeige im Dashboard.
- **Key-Rotation:** Keys können durch den Kunde jederzeit rotiert werden.
- **JWT-Tokens:** Optional Bearer-Token-Authentication für zusätzliche Sicherheit.
- **Rate Limiting:** Implementierung von Rate-Limiting-Mechanismen zur Abwehr von DoS-Angriffen und Überlastung (dynamische Limits basierend auf Systemlast und Tarif)

1.3 Zugriffskontrolle (Interne Systeme)

- **Principle of Least Privilege:** Nur autorisierte Mitarbeiter haben Zugriff auf Produktionssysteme.
- **Kubernetes RBAC:** Rollen- und Attributbasierte Zugriffskontrolle in der Container-Orchestrierung.
- **VPN-Zugang:** Alle remote-administrativen Zugriffe erfolgen über verschlüsselte Verbindungen (z. B. SSH mit Public-Key-Authentication, VPN oder TLS-gesicherte Konsolen)
- **MFA (Multi-Faktor-Authentifizierung):** Erzwungen für alle administrativen Zugriffe auf Cloud-Konsolen und Code-Repositories (GitHub, etc.).
- **SSH-Keys:** Nur public-key-basierte SSH-Authentifizierung; Passwort-SSH ist deaktiviert.

1.4 Daten-Isolation

- **Row Level Security (RLS):** Datenbank-Policies stellen sicher, dass jede Organisation nur ihre eigenen Daten sieht.
- **Organisationsbasiertes Mapping:** User → Org-Zuordnung ist in der Zugriffslogik verankert.
- **Credit-System:** Ressourcennutzung ist an organisationsspezifische Credits gebunden.

1.5 Vertraulichkeitsverpflichtung

- Alle Mitarbeiter und Subunternehmer unterzeichnen schriftliche Vertraulichkeitserklärungen (NDAs) vor Zugriff auf Kundendaten.

---

2. INTEGRITÄT (WEITERGABEKONTROLLE, EINGABEKONTROLLE)

2.1 Datentrennung

- **Logische Trennung:** Kundendaten sind logisch nach Organisationen getrennt und können nicht versehentlich vermischt werden.

2.2 Eingabekontrolle & Audit-Logging

- **Administrativer Zugriff:** Jeder administrative Zugriff wird geloggt (Zeitstempel, Admin-ID, durchgeführte Aktion).
- **API-Audit-Logs:** Alle API-Requests werden protokolliert mit:
  - Zeitstempel
  - User-ID / Org-ID
  - API-Key-ID (gehashed)
  - Model-ID / Endpunkt
  - Request-Größe
  - HTTP-Status-Code
  - Verarbeitungszeit
- **Inhalts-Datenschutz:** Input-Texte und generiertes Audio werden NICHT in Logs gespeichert (nur Metadaten).
- **Log-Aufbewahrung:** Logs werden mindestens 90 Tage aufbewahrt und anschließend archiviert oder gelöscht.

2.3 Integrität von Verbindungen

- **TLS mit Integritätsprüfung:** TLS stellt sicher, dass Daten nicht unterwegs manipuliert werden (HMAC).

---

3. VERFÜGBARKEIT UND BELASTBARKEIT (DISASTER RECOVERY, BACKUP, HOCHVERFÜGBARKEIT)

3.1 Redundanz

- **Load Balancing:** Traffic wird automatisch auf mehrere Server verteilt.

3.2 Backups

- **Regelmäßige Backups:** Tägliche inkrementelle Backups und wöchentliche vollständige Backups.
- **Geo-Redundanz:** Backups werden an mehreren geografischen Orten gespeichert (EU-Rechenzentren).
- **Verschlüsselung:** Alle Backups werden mit AES-256 verschlüsselt.
- **Testverfahren:** Backup-Restore-Tests werden monatlich durchgeführt.
- **Aufbewahrungsdauer:** Backups werden 30 Tage aufbewahrt; längere Aufbewahrung auf Anforderung.

3.3 Monitoring & Alerting

- **24/7 Monitoring:** Automatisierte Überwachung von Systemmetriken (CPU, Memory, Disk, Network, Error-Rates).
- **Automated Alerts:** Kritische Events triggern sofortige Benachrichtigungen an KugelAudio-Betriebsteam.
- **Uptime-Ziel:** 99.5% Verfügbarkeit (SLA, siehe Hauptvertrag).

- **Status Page:** Öffentliche Status-Seite zeigt Systemverfügbarkeit in Echtzeit.

3.4 Skalierbarkeit

- **Auto-Scaling:** GPU-Cluster skalieren automatisch basierend auf Nachfrage (Kubernetes HPA).
- **Rate Limiting:** Schützt vor Überlastung durch Limiting von RPS und gleichzeitigen Verbindungen (siehe 1.2).
- **Queue Management:** Bei Spitzenlast werden Anfragen in Warteschlangen gepuffert und Fair-Share-mäßig verarbeitet.

---

4. DATENSPEICHERUNG UND LÖSCHUNG

4.1 RAM-Only für Audio/Text

- **Input-Texte:** Werden ausschließlich im RAM während der Verarbeitung gehalten, nicht auf Festplatte geschrieben.
- **Generiertes Audio:** Wird gestreamt (WebSocket) an den Client und nicht persistent gespeichert (außer wenn vom Kunden explizit angefordert).
- **Automatische Freigabe:** Nach Beendigung des Requests wird Speicher sofort freigegeben.

4.2 Voice References (Stimm-Samples)

- **Speicherort:** On-Premises in EU-Rechenzentren (Verda/Hetzner).
- **Verschlüsselung:** Verschlüsselt auf Festplatte (Encryption at Rest).
- **Zugriffskontrolle:** Nur der Org-Owner und autorisierte Keys können Samples abrufen.
- **Löschung:** Auf Kundenanforderung oder nach Vertragsende werden Voice References gelöscht.

4.3 Billing- und Metadaten

- **Aufbewahrungsdauer:** Entsprechend deutschen Aufbewahrungsfristen (6-10 Jahre für Geschätsunterlagen, je nach Art).
- **Anonymisierung:** Nach Aufbewahrungsfrist werden personenbezogene Daten anonymisiert oder gelöscht.

---

5. DATENSCHUTZ DURCH DESIGN UND STANDARD

5.1 Privacy by Design

- **Minimale Datenverarbeitung:** Nur die minimal erforderlichen Daten werden verarbeitet.

- **Pseudonymisierung:** User-IDs werden intern durch Hashes dargestellt; echte Nutzeridentitäten werden nicht mit Request-Daten verknüpft.
- **Datensparsamkeit:** Keinen Datenverkauf, keine Sekundärnutzung ohne explizite Zustimmung.

5.2 Datenschutzerklärung & Transparenz

- KugelAudio stellt klare Dokumentation zur Datenverarbeitung bereit (siehe Kundendokumentation).
- Jeder Kunde kann einsehen, welche Daten über welche Zeiträume gespeichert werden.

---

6. SICHERHEITSUPDATES UND PATCHING

- **Updates**: Sicherheitsrelevante Patches werden zeitnah nach Verfügbarkeit und erfolgreicher interner Prüfung eingespielt.
- **Kritische Lücken:** Kritische Sicherheitslücken werden priorisiert behandelt und schnellstmöglich geschlossen.
- **Wartungsfenster:** Notwendige Wartungsarbeiten werden, soweit möglich, außerhalb der Hauptgeschäftszeiten durchgeführt.

---

7. INCIDENT RESPONSE & FORENSICS

- **Incident-Management:** Es existiert ein definierter Prozess zur Meldung und Bearbeitung von Sicherheitsvorfällen.
- **Reaktionszeiten:** Die Reaktion auf Sicherheitsvorfälle erfolgt innerhalb der im Hauptvertrag (SLA) vereinbarten Servicezeiten.
- **Analyse:** Nach Abschluss eines kritischen Vorfalls erfolgt eine Analyse zur Vermeidung zukünftiger Risiken.

---

8. EXTERNE AUDITS & ZERTIFIZIERUNGEN

- **Interne Audits:** KugelAudio führt regelmäßig (mindestens jährlich) interne Sicherheitsüberprüfungen und Reviews der technischen Maßnahmen durch.
- **Externe Zertifizierung:** Eine Zertifizierung nach internationalen Industriestandards (z. B. SOC 2 Type II oder ISO 27001) wird angestrebt und ist Teil der langfristigen Sicherheits-Roadmap. Zum aktuellen Zeitpunkt liegen diese Zertifikate noch nicht vor.
- **Transparenz:** Auf Anforderung stellt KugelAudio dem Auftraggeber die Ergebnisse der internen Sicherheitsreviews (in zusammengefasster Form) zur Verfügung.

ANLAGE 2: UNTERAUFTRAGSVERARBEITER (SUB-PROCESSOR)

A) KERN-INFRASTRUKTUR (Verarbeitung von Audio- & Textdaten)

Diese Dienstleister haben direkten Kontakt mit den Sprachverarbeitungsdaten (Texte, Audio, Voice-Samples).

Dienstleister	Sitz	Leistung	Verarbeitungsort	Rechtsgrundlage
Verda AI (GPU Cloud)	EU (Finnland)	GPU-Inferenz für TTS/STT-Modelle, Hosting	Primär EU (EWR); vereinzelt Drittlandtransfers nur gem. SCCs	AVV (Data Processing Terms)
Hetzner Online GmbH	Deutschland (Gunzenhausen)	GPU-Server und Infrastruktur für KI-Modelle	Deutschland (EU)	Subvertrag mit Datenschutzverpflichtung

---

B) BUSINESS- & SUPPORT-INFRASTRUKTUR

Diese Dienstleister verarbeiten Business-Daten (Account-Info, Zahlungen, Logs) – haben aber KEINEN Zugriff auf Audio/Text-Inhalte oder Voice Samples.

Dienstleister	Sitz	Leistung	Verarbeitungsort	Rechtsgrundlage	Datenfluss
Vercel Inc.	USA	Frontend / Web-Application Hosting	USA / Global CDN	Subvertrag + Data Privacy Framework / SCC	Website-Besucherdaten, anonymisierte Session-Daten
Functional Software, Inc. (Sentry)	USA	Error & Performance Monitoring	USA	Subvertrag + Data Privacy Framework / SCC	Technische Error-Logs (keine Audio/Text-Payloads)

ERKLÄRUNGEN ZU DATENFLÜSSEN

Audio- und Text-Sicherheit (nicht bei USA-Providern)

Input-Texte und generiertes Audio verlassen NIEMALS die EU-Infrastruktur. Sie kommen nicht in Kontakt mit USA-Subunternehmern.

```
None
Nutzer-Input (Text/Audio)
    ↓
HTTPS/WSS → KugelAudio API (EU)
    ↓
Verda/Hetzner GPU (EU) ← TTS-Verarbeitung findet HIER statt
    ↓
Audio-Stream → Nutzer via WSS
    ↓
[Audio wird nicht gespeichert oder an Dritte weitergegeben]
```

Business-Daten (teilweise in USA)

```
None
Business-Daten (teilweise in USA)
Kunde registriert sich
↓
E-Mail, Name → Supabase Datenbank (Self-Hosted in EU)
↓
Account-Status & Auth → Vercel (USA/Global) für Login-Session
↓
[Zahlungsdaten werden direkt vom Zahlungsanbieter (eigener Verantwortlicher)
verarbeitet und berühren diesen AVV nicht]
```

Internationales Datenschutzniveau

Für Subunternehmer in den USA (Drittländer) gelten folgende Sicherungen gemäß Art. 46 DSGVO:

1. **EU-U.S. Data Privacy Framework (DPF) oder Standardvertragsklauseln (SCC)**: Die eingesetzten US-Dienstleister (Vercel, Sentry) werden durch Standardvertragsklauseln und/oder Teilnahme am DPF abgesichert

2. **Standard Contractual Clauses (SCCs):**

    - Vercel (SCC vorhanden)

- Sentry (SCC vorhanden)

3. **Supplementary Measures:**

    - Encryption at Rest / in Transit
    - Strikte Zugriffskontrolle (nur KugelAudio-Mitarbeiter)
    - Keine weitergabe an US-Behörden ohne Benachrichtigung

ÄNDERUNGEN AN DER LISTE

Der Prozess zur Hinzuziehung oder zum Austausch von Subunternehmern (inkl. Benachrichtigungspflichten und Widerspruchsfristen) richtet sich nach den Bestimmungen in § 6 dieses Vertrags

---

„Dieser Vertrag wird elektronisch geschlossen und ist auch ohne handschriftliche Unterschrift gültig. Mit der Zustimmung zu den Nutzungsbedingungen (Terms of Service) oder der Nutzung der Plattform gilt dieser Vertrag als abgeschlossen.“

Stand: 23.01.2026