AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO, Variante: EU AVV

DATA PROCESSING AGREEMENT (DPA)

pursuant to Art. 28 GDPR, Variant: EU DPA

VERTRAGSPARTEIEN

Auftraggeber (Verantwortlicher):

[Name / Firma]
[Adresse]
[Land]

Auftragnehmer (Auftragsverarbeiter):
KugelAudio GmbH
Rosenthaler Str. 36
10178 Berlin
Deutschland
Vertreten durch die Geschäftsführer: Kajo Kratzenstein, Viktor Presber

Handelsregister: Amtsgericht Charlottenburg, HRB 277989 B

CONTRACTING PARTIES

Controller (“Customer”):

[Name / Company]
[Address]
[Country]

Processor:
KugelAudio GmbH
Rosenthaler Str. 36
10178 Berlin
Germany
Represented by the managing directors: Kajo Kratzenstein, Viktor Presber

Commercial register: Local Court of Charlottenburg (Berlin), 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 GmbH (im Folgenden „KugelAudio“).

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

§ 1 SCOPE

(1) This agreement governs the processing of personal data on behalf of the controller pursuant to Art. 28 GDPR between the controller (hereinafter the “Customer”) and the processor KugelAudio GmbH (hereinafter “KugelAudio”).

(2) This agreement forms an integral part of the service agreement / terms of service between the parties (hereinafter the “Main Agreement”).

---

§ 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.

§ 2 SUBJECT MATTER AND DURATION OF PROCESSING

(1) Subject matter: KugelAudio provides an AI-powered speech processing platform (speech-to-speech / text-to-speech) via API and web interfaces, including hosting of the required infrastructure. All processing is carried out exclusively on the Customer's instructions and in accordance with the service logic defined in the Main Agreement.

(2) Duration: Processing begins when this agreement enters into force and continues for the duration of the service provision. If the Main Agreement is terminated, this processing relationship ends no later than 30 days after notice of termination. Provisions on data deletion apply independently.

§ 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 der 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.

§ 3 NATURE, PURPOSE AND SCOPE OF PROCESSING

(1) Processing operations: KugelAudio carries out the following processing operations:

– Collection and reading of audio data (voice recordings)

– Processing of text data (input prompts, transcripts)

– Synthesis and conversion using AI models (TTS/STT)

– Storage of voice references (voice cloning samples), where provided by the Customer

– Short-term, temporary storage in RAM during processing

– Streaming of audio output to the Customer's end users

– Creation of technical logs and usage metadata

(2) Purpose:

– Enabling real-time voice interactions for the Customer's end applications

– Provision of the voice AI services under the Main Agreement

– Training and inference of AI voice models (where separately commissioned)

– Technical monitoring, support and billing

(3) Categories of data:

– Audio data: voice recordings of the Customer's end users

– Text data: input prompts, transcripts, configuration parameters

– Metadata: timestamps, user IDs, organisation IDs, model IDs, API key IDs, request sizes, processing times

– Voice references: optionally uploaded voice samples for voice cloning

– Technical logs: error logs, request logs (no content payloads)

(4) Data subjects:

– Customers and users of the Customer

– Employees of the Customer (insofar as they interact with KugelAudio services)

(5) Categories of recipients: see § 6 (sub-processors) and Annex 2.

§ 3A ZERO DATA RETENTION (ZDR) FÜR INHALTSDATEN

(1) Zero Data Retention für Inhaltsdaten: KugelAudio speichert vom Auftraggeber übermittelte oder im Rahmen der Leistungserbringung erzeugte Inhaltsdaten, insbesondere Text-, Audio- und Sprachdaten, Prompts und Transkripte, nicht über die Dauer des jeweiligen Verarbeitungsvorgangs hinaus. Solche Inhaltsdaten werden ausschließlich flüchtig im Arbeitsspeicher (RAM) verarbeitet und nach Abschluss der jeweiligen Anfrage automatisch und unverzüglich gelöscht.

(2) Sachlicher Anwendungsbereich (Klarstellung): Zero Data Retention gilt ausschließlich für Inhaltsdaten, d. h. für die vom Auftraggeber übermittelten oder für ihn erzeugten Text-, Audio- und Sprachdaten, Prompts und Transkripte. Nicht erfasst sind a) Account-, Stamm- und Vertragsdaten (z. B. Nutzer- und Organisationsdaten, Authentifizierungsdaten, Projektkonfigurationen), b) technische Metadaten ohne Inhaltsbezug (z. B. Zeitstempel, Anfragegrößen, API-Key-IDs, Verarbeitungszeiten, Fehler- und Zugriffsprotokolle ohne Inhaltsdaten) sowie c) Abrechnungs- und Rechnungsdaten, die gesetzlichen Aufbewahrungspflichten unterliegen (insbesondere § 147 AO, § 257 HGB). Diese Daten dürfen von KugelAudio gespeichert und für die Dauer des Vertragsverhältnisses bzw. der gesetzlichen Aufbewahrungsfristen aufbewahrt werden.

(3) Keine persistente Speicherung oder Protokollierung: Eine persistente Speicherung, Archivierung, Protokollierung oder Sicherung von Inhaltsdaten findet nicht statt. Inhaltsdaten werden insbesondere nicht in Logs, Backups oder Monitoring-Systemen gespeichert.

(4) Ausnahmen von Zero Data Retention: Über die in Absatz 2 genannten, von vornherein nicht erfassten Datenkategorien hinaus gilt Zero Data Retention nicht für Voice References, soweit diese vom Auftraggeber aktiv und ausdrücklich für die Nutzung bestimmter Funktionen (z. B. Voice Cloning) bereitgestellt werden; deren Speicherung und Löschung richtet sich nach § 7.

(5) Keine Nutzung zu Trainings- oder Analysezwecken: Inhaltsdaten des Auftraggebers werden nicht für Training, Analyse, Qualitätsverbesserung oder sonstige Sekundärzwecke verwendet.

(6) Flüchtige technische Zwischenspeicherung: Kurzlebige, technisch notwendige Zwischenspeicherungen von Inhaltsdaten (z. B. In-Memory-Queues und Streaming-Puffer) stellen keine Speicherung im Sinne dieses Abschnitts dar, sofern die Daten nach Abschluss des jeweiligen Verarbeitungsschritts automatisch gelöscht werden. Eine Protokollierung oder Aufbewahrung von Inhaltsdaten zu Support- oder Debugging-Zwecken erfolgt nur mit vorheriger ausdrücklicher Zustimmung des Auftraggebers und wird nach Zweckerfüllung gelöscht.

§ 3A ZERO DATA RETENTION (ZDR) FOR CONTENT DATA

(1) Zero Data Retention for content data: KugelAudio does not store content data transmitted by the Customer or generated in the course of service provision, in particular text, audio and voice data, prompts and transcripts, beyond the duration of the respective processing operation. Such content data is processed exclusively transiently in working memory (RAM) and is deleted automatically and without delay upon completion of the respective request.

(2) Material scope (clarification): Zero Data Retention applies exclusively to content data, i.e. the text, audio and voice data, prompts and transcripts transmitted by the Customer or generated on its behalf. It does not cover a) account, master and contract data (e.g. user and organisation data, authentication data, project configurations), b) technical metadata without content reference (e.g. timestamps, request sizes, API key IDs, processing times, error and access logs containing no content data), or c) billing and invoicing data subject to statutory retention obligations (in particular § 147 German Fiscal Code (AO), § 257 German Commercial Code (HGB)). KugelAudio may store such data and retain it for the duration of the contractual relationship or the statutory retention periods respectively.

(3) No persistent storage or logging: No persistent storage, archiving, logging or backup of content data takes place. In particular, content data is not stored in logs, backups or monitoring systems.

(4) Exclusions from Zero Data Retention: In addition to the categories of data not covered in the first place under paragraph 2, Zero Data Retention does not apply to voice references, where these are actively and expressly provided by the Customer for the use of specific functions (e.g. voice cloning); their storage and erasure is governed by § 7.

(5) No use for training or analysis purposes: The Customer's content data is not used for training, analysis, quality-improvement or other secondary purposes.

(6) Transient technical buffering: Short-lived, technically necessary buffering of content data (e.g. in-memory queues and streaming buffers) does not constitute storage within the meaning of this section, provided the data is deleted automatically once the respective processing step completes. Any logging or retention of content data for support or debugging purposes takes place only with the Customer's prior express consent and is deleted once the purpose is fulfilled.

§ 4 PFLICHTEN DES AUFTRAGGEBERS

(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.

§ 4 OBLIGATIONS OF THE CUSTOMER

(1) The Customer undertakes to instruct KugelAudio only in accordance with the terms of this agreement and applicable data protection laws.

(2) The Customer bears full responsibility for ensuring that the data transmitted to KugelAudio was collected lawfully and that the processing is legally permissible (basis: consent, contract, legal obligation or similar).

(3) The Customer warrants that it has obtained all necessary consents from the data subjects or that the processing can be based on other legal grounds.

---

§ 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.

(1a) Hinweispflicht bei rechtswidrigen Weisungen: KugelAudio informiert den Auftraggeber unverzüglich, wenn es der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). KugelAudio ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

(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)

§ 5 OBLIGATIONS OF THE PROCESSOR (KUGELAUDIO)

(1) Processing on instructions: KugelAudio processes personal data exclusively on the Customer's documented instructions and in accordance with the functionality described in the Main Agreement. Additional processing takes place only with prior written approval.

(1a) Duty to flag unlawful instructions: KugelAudio informs the Customer without undue delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions (Art. 28(3) sentence 3 GDPR). KugelAudio is entitled to suspend execution of the instruction concerned until it is confirmed or amended by the Customer.

(2) Confidentiality: KugelAudio ensures that only authorised persons have access to the Customer's data. All employees and subcontractors are bound to confidentiality in writing.

(3) Security measures: KugelAudio implements and maintains the technical and organisational measures (TOMs) listed in Annex 1. In the event of security vulnerabilities, KugelAudio notifies the Customer without undue delay.

(4) Data separation: Data processed under this agreement is logically and technically separated from other data sets.

(5) No copies without the Customer's knowledge: Copies or duplicates are not created, except for:

- Technically necessary, temporary copies in RAM during processing
- Backups pursuant to § 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) Backups: KugelAudio performs regular, encrypted backups of master and configuration data and documents them. Backups are retained in accordance with applicable retention periods.

(7) Proof of compliance: On the Customer's request, KugelAudio provides evidence of compliance with its security obligations, in particular:

– Documentation of the technical and organisational measures

– Evidence must be provided on request within 30 working days at the latest

(8) Regular review: KugelAudio reviews the effectiveness of the security measures at least annually.

---

§ 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 mindestens vier (4) Wochen vor der Hinzuziehung oder dem Austausch eines Subunternehmers (via E-Mail oder Dashboard-Notifikation). Ist der Austausch eines Subunternehmers aus wichtigen Gründen der Sicherheit oder der Aufrechterhaltung des Betriebs erforderlich und eine vorherige Ankündigung nicht zumutbar, kann KugelAudio den Subunternehmer sofort austauschen und informiert den Auftraggeber unverzüglich nachträglich; das Widerspruchsrecht des Auftraggebers bleibt unberührt.

(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

§ 6 SUB-PROCESSORS (SUBCONTRACTORS)

(1) General authorisation: The Customer grants KugelAudio general authorisation to engage further processors (sub-processors). The sub-processors currently engaged are listed in Annex 2.

(2) Notification obligation: KugelAudio notifies the Customer at least four (4) weeks before engaging or replacing a sub-processor (via email or dashboard notification). Where the replacement of a sub-processor is necessary for important reasons of security or service continuity and advance notice is not reasonably possible, KugelAudio may replace the sub-processor immediately and will notify the Customer without undue delay afterwards; the Customer's right to object remains unaffected.

(3) Right to object: The Customer may object in writing to the engagement or replacement of a sub-processor within 4 weeks of receipt of the notification. The objection must be based on and substantiated by a material data protection concern. If no timely and substantiated objection is made, the change is deemed approved.

(4) Contractual guarantees: Each sub-processor is contractually bound to comply with data protection standards at least equivalent to those agreed in this agreement. On request, KugelAudio grants the Customer access to the relevant contractual terms.

(5) Liability: KugelAudio remains fully liable to the Customer for the performance of the obligations by its sub-processors.

(6) Further subcontracting (chain of guarantees): The processor contractually obliges its direct sub-processors to pass on the data protection provisions of this agreement (in particular the requirements of Art. 28(4) GDPR) to their own sub-processors and to engage further sub-processors only under the following conditions: (a) processing of customer

und weitere Unterauftragnehmer nur unter folgenden Bedingungen einzusetzen: (a) Verarbeitung von Kundendaten ausschließlich innerhalb der EU; (b) Abschluss eines schriftlichen AVV mit einem Schutzniveau, das diesem Vertrag mindestens gleichwertig ist. KugelAudio stellt dem Auftraggeber auf Anfrage innerhalb von zehn (10) Geschäftstagen eine aktuelle Liste der bekannten Sub-Subunternehmer zur Verfügung. Verda hat schriftlich bestätigt, dass Kundendaten ausschließlich durch Verda selbst verarbeitet werden (Bestätigung vom 04.03.2026). Eine gesonderte Genehmigung durch den Auftraggeber für die Hinzuziehung weiterer Unterauftragnehmer durch die Unterauftragnehmer (Sub-Sub-Unternehmer) ist nicht erforderlich, sofern die vorstehenden Bedingungen eingehalten werden und das Datenschutzniveau gewahrt bleibt.

data exclusively within the EU; (b) a written DPA providing a level of protection at least equivalent to this agreement. Upon request, KugelAudio provides the Customer with a current list of known sub-sub-processors within ten (10) business days. Verda has confirmed in writing that customer data is processed exclusively by Verda itself (confirmation dated 4 March 2026). Separate approval by the Customer for the engagement of further sub-processors by the sub-processors (sub-sub-processors) is not required, provided the above conditions are met and the level of data protection is maintained.

§ 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 oder -rückgabe nach Vertragsende: Nach Beendigung der Auftragsverarbeitung oder auf Wunsch des Auftraggebers werden alle im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder gelöscht oder an den Auftraggeber zurückgegeben und anschließend gelöscht (Art. 28 Abs. 3 lit. g DSGVO), sofern keine gesetzliche Aufbewahrungspflicht besteht. Ausgenommen sind anonymisierte oder verschlüsselte Archivkopien, die für historische oder gesetzliche Compliance-Anforderungen notwendig sind.

§ 7 RECTIFICATION, ERASURE AND RESTRICTION OF DATA

(1) Implementation of instructions: KugelAudio carries out all instructions from the Customer to rectify, erase or restrict data without undue delay. Instructions that go beyond the contractually agreed service or functionality, or that require technical changes to the platform, require a separate agreement on cost allocation and feasibility.

(2) Time frame: Instructions are carried out within 5 working days of receipt, unless a longer period is technically required or legally prescribed.

(3) Evidence: KugelAudio documents the measures taken and confirms them to the Customer.

(4) Deletion or return after contract end: Upon termination of the processing or at the Customer's request, all data processed under this agreement is, at the Customer's choice, either deleted or returned to the Customer and subsequently deleted (Art. 28(3)(g) GDPR), unless a statutory retention obligation exists. Anonymised or encrypted archive copies required for historical or statutory compliance purposes are exempt.

§ 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

§ 8 DATA SECURITY INCIDENTS

(1) Notification obligation: KugelAudio notifies the Customer of any personal data breach without undue delay, and no later than 72 hours after discovery.

(2) Content of the notification: The notification includes:

- Description of the security incident

– 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.

– Affected data and data subjects (where known)

– Likely consequences

– Remedial measures taken and planned

– Contact person at KugelAudio for further information

(3) Notification support: KugelAudio supports the Customer in fulfilling its notification obligations towards supervisory authorities (Art. 33 GDPR) and data subjects (Art. 34 GDPR).

(4) Documentation: All incidents are documented.

§ 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) Recht auf Datenübertragbarkeit: Falls der Auftraggeber die Portabilität von Daten verlangt, stellt KugelAudio diese in einem strukturierten, gängigen, maschinenlesbaren Format bereit.

§ 9 DATA SUBJECT RIGHTS

(1) Support with access requests: On the Customer's instructions, KugelAudio cooperates in fulfilling access, erasure, rectification and other data subject rights requests pursuant to Art. 15-22 GDPR.

(2) Information obligation: KugelAudio provides all information necessary for the Customer to comply with its obligations under Art. 12-14 GDPR (informing data subjects).

(3) Right to data portability: If the Customer requests data portability, KugelAudio provides the data in a structured, commonly used, machine-readable format.

§ 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).

§ 10 AUDIT RIGHTS OF THE CUSTOMER

(1) Security evidence: KugelAudio demonstrates compliance with the technical and organisational measures primarily by providing current self-declarations, documentation of security concepts, or reports on internal security reviews. If KugelAudio obtains external certifications in the future (e.g. SOC 2, ISO 27001), such reports may replace or supplement the aforementioned evidence.

(2) On-site inspections: An on-site audit is only permissible if the Customer demonstrates that the evidence referred to in paragraph 1 (documentation, reports) is insufficient to demonstrate compliance, or if mandatory legal requirements so demand. Such inspections must be announced in writing with at least four (4) weeks' notice and must not disrupt business operations.

(3) Costs: The Customer bears all costs of the inspection (including the costs of external auditors). In addition,

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.

KugelAudio is entitled to charge its own personnel expenses for accompanying the inspection at reasonable, market-standard hourly rates, unless the audit reveals material, intentional or grossly negligent violations by KugelAudio.

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

(4) Sub-processors: KugelAudio grants access to the data protection-relevant parts of its contracts with sub-processors. Commercial terms or trade secrets may be redacted.

§ 11 DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)

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

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

§ 11 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

(1) KugelAudio supports the Customer in carrying out a data protection impact assessment (DPIA) pursuant to Art. 35 GDPR where high-risk processing is involved.

(2) KugelAudio provides the necessary information about its technical and organisational measures.

§ 12 DATENSCHUTZBEAUFTRAGTER

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

§ 12 DATA PROTECTION OFFICER

Where required, KugelAudio appoints a data protection officer and informs the Customer of the officer's contact details.

§ 13 INTERNATIONALE DATENÜBERTRAGUNGEN (EU-ONLY HOSTING)

(1) EU-Verarbeitung: Sämtliche Verarbeitungsvorgänge, einschließlich Audio- und Textdaten, Voice References sowie Business-Daten (Account-Informationen, Abrechnungsdaten, technische Logs), erfolgen ausschließlich auf Servern und in Verarbeitungsregionen innerhalb der EU (insbesondere Deutschland, Finnland und Frankreich); die eingesetzten Infrastruktur-Anbieter sind in Anlage 2 A aufgeführt.

(2) Dienstleister mit Sitz außerhalb der EU: In dieser Vertragsvariante wird kein Subunternehmer mit Sitz oder Muttergesellschaft in den USA eingesetzt. Der einzige außerhalb der EU ansässige Subunternehmer ist Supabase Pte. Ltd. (Singapur); seine Verarbeitungsregion ist vertraglich auf die EU festgelegt, und er verarbeitet ausschließlich Account- und Abrechnungsdaten. Für einen etwaigen verbleibenden Drittlandzugriff (z. B. Remote-Support) gelten als Transfermechanismus gemäß Art. 46 DSGVO die EU-Standardvertragsklauseln (SCC).

(3) Sicherheitsgewährleistung: KugelAudio informiert den Auftraggeber über alle Länderübermittlungen und die

§ 13 INTERNATIONAL DATA TRANSFERS (EU-ONLY HOSTING)

(1) EU processing: All processing operations, including audio and text data, voice references, and business data (account information, billing data, technical logs), take place exclusively on servers and in processing regions within the EU (in particular Germany, Finland and France); the infrastructure providers engaged are listed in Annex 2 A.

(2) Providers established outside the EU: No sub-processor established in, or with a parent company in, the USA is engaged under this contract variant. The only sub-processor established outside the EU is Supabase Pte. Ltd. (Singapore); its processing region is contractually pinned to the EU and it processes account and billing data only. For any residual third-country access (e.g. remote support), EU Standard Contractual Clauses (SCCs) apply as the transfer mechanism pursuant to Art. 46 GDPR.

(3) Safeguards: KugelAudio informs the Customer of all cross-border transfers and the safeguards applied. Under

angewendeten Schutzmaßnahmen. Eine Verlagerung von Verarbeitungsorten außerhalb der EU erfolgt im Rahmen dieser Vertragsvariante nicht ohne vorherige ausdrückliche Zustimmung des Auftraggebers.

this contract variant, processing locations are not moved outside the EU without the Customer's prior express consent.

§ 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.

§ 14 COSTS AND CONTRACT TERM

(1) Costs: The costs of the processing are included in the fees of the Main Agreement. Additional audits or compliance measures may be charged separately.

(2) Termination: This agreement runs in parallel with the Main Agreement. If the Main Agreement is terminated, this processing relationship also ends.

§ 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 Textform (§ 126b BGB; E-Mail genügt). KugelAudio kann diesen Vertrag mit einer Vorankündigung von mindestens vier (4) Wochen ändern, soweit dies zur Umsetzung von Rechtsänderungen, aufsichtsbehördlichen Vorgaben oder Änderungen der Dienste erforderlich ist. Senkt eine Änderung das Datenschutzniveau wesentlich ab, kann der Auftraggeber innerhalb von vier (4) Wochen nach Zugang der Ankündigung schriftlich widersprechen; in diesem Fall wird die Änderung ihm gegenüber nicht wirksam und die Parteien bemühen sich um eine einvernehmliche Lösung; gelingt dies nicht, kann jede Partei die betroffenen Dienste mit angemessener Frist kündigen.

(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 Berlin.

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

(6) Sprachfassungen: Dieser Vertrag ist in deutscher und englischer Sprache abgefasst. Bei Widersprüchen zwischen den Sprachfassungen ist die deutsche Fassung maßgeblich.

§ 15 FINAL PROVISIONS

(1) Term: This agreement takes effect upon conclusion of the Main Agreement and runs for the entire duration of the business relationship.

(2) Amendments: Amendments to this agreement require text form (Section 126b German Civil Code; email suffices). KugelAudio may amend this agreement with at least four (4) weeks' prior notice where necessary to reflect changes in law, supervisory guidance or the services. If an amendment materially reduces the level of data protection, the Customer may object in writing within four (4) weeks of the notice; in that case the amendment does not take effect vis-à-vis the Customer, and the parties shall seek a mutually acceptable solution; failing that, either party may terminate the affected services with reasonable notice.

(3) Severability: If any provision of this agreement is invalid, the remainder of the agreement remains valid. The parties will agree on a permissible provision with a comparable purpose.

(4) Governing law: This agreement is governed by German law. The place of jurisdiction is Berlin, Germany.

(5) Data protection laws: Compliance with the GDPR, the German Federal Data Protection Act (BDSG) and other applicable data protection laws is mandatory.

(6) Language versions: This agreement is drawn up in German and English. In the event of discrepancies between the language versions, the German version prevails.

ANLAGEN

ANNEXES

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 Kunden 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

ANNEX 1: TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

1. CONFIDENTIALITY (PHYSICAL, SYSTEM AND DATA ACCESS CONTROL)

1.1 Transport encryption

– HTTPS/TLS: All web requests are encrypted via TLS 1.2 or higher.

– WSS (WebSocket Secure): Real-time audio streaming runs over encrypted WebSocket connections (wss://).

– Certificates: Let's Encrypt or equivalent trusted certificate authorities. Automatic renewal.

– SSL redirect: HTTP requests are automatically redirected to HTTPS.

1.2 Authentication & API security

– API keys: API endpoints are accessible only with validated API keys. Keys are truncated when displayed in the dashboard.

– Key rotation: Keys can be rotated by the Customer at any time.

– JWT tokens: Optional bearer token authentication for additional security.

– Rate limiting: Rate limiting mechanisms to defend against DoS attacks and overload (dynamic limits based on system load and plan).

1.3 Access control (internal systems)

– Principle of least privilege: Only authorised employees have access to production systems.

– Kubernetes RBAC: Role- and attribute-based access control in the container orchestration.

– VPN access: All remote administrative access is via encrypted connections (e.g. SSH with public-key authentication, VPN, or TLS-secured consoles).

– MFA (multi-factor authentication): Enforced for all administrative access to cloud consoles and code repositories (GitHub, etc.).

– SSH keys: Public-key-based SSH authentication only; password SSH is disabled.

1.4 Data isolation

– Row level security (RLS): Database policies ensure

sicher, dass jede Organisation nur ihre eigenen Daten sieht.

– Organisationsbasiertes Mapping: User-zu-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.

each organisation only sees its own data.

– Organisation-based mapping: User-to-organisation assignment is anchored in the access logic.

– Credit system: Resource usage is tied to organisation-specific credits.

1.5 Confidentiality commitment

– All employees and subcontractors sign written confidentiality agreements (NDAs) before accessing customer data.

---

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).

2. INTEGRITY (TRANSFER CONTROL, INPUT CONTROL)

2.1 Data separation

– Logical separation: Customer data is logically separated by organisation and cannot be accidentally mixed.

2.2 Input control & audit logging

– Administrative access: Every administrative access is logged (timestamp, admin ID, action performed).

– API audit logs: All API requests are logged with: timestamp, user ID / org ID, API key ID (hashed), model ID / endpoint, request size, HTTP status code, processing time.

– Content privacy: Input texts and generated audio are NOT stored in logs (metadata only).

– Log retention: Logs are retained for at least 90 days and then archived or deleted.

2.3 Connection integrity

– TLS with integrity verification: TLS ensures data is not tampered with in transit (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

3. AVAILABILITY AND RESILIENCE (DISASTER RECOVERY, BACKUP, HIGH AVAILABILITY)

3.1 Redundancy

– Load balancing: Traffic is automatically distributed across multiple servers.

3.2 Backups

– Regular backups: Daily incremental backups and

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 das 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.

weekly full backups.

– Geo-redundancy: Backups are stored in multiple geographic locations (EU data centres).

– Encryption: All backups are encrypted with AES-256.

– Test procedures: Backup restore tests are performed monthly.

– Retention: Backups are retained for 30 days; longer retention on request.

3.3 Monitoring & alerting

– 24/7 monitoring: Automated monitoring of system metrics (CPU, memory, disk, network, error rates).

– Automated alerts: Critical events trigger immediate notifications to the KugelAudio operations team.

– Uptime target: 99.5% availability (SLA, see Main Agreement).

– Status page: Public status page shows system availability in real time.

3.4 Scalability

– Auto-scaling: GPU clusters scale automatically based on demand (Kubernetes HPA).

– Rate limiting: Protects against overload by limiting RPS and concurrent connections (see 1.2).

– Queue management: Under peak load, requests are buffered in queues and processed fair-share.

---

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: S3-kompatibler Object Storage in EU-Rechenzentren — Hetzner Object Storage (Deutschland) und Scaleway Object Storage (Frankreich); Verarbeitung in EU-Rechenzentren (Verda/Hetzner).

4. DATA STORAGE AND DELETION

4.1 RAM-only for audio/text

– Input texts: Held exclusively in RAM during processing, never written to disk.

– Generated audio: Streamed (WebSocket) to the client and not persistently stored (unless explicitly requested by the Customer).

– Automatic release: Memory is released immediately after the request completes.

4.2 Voice references (voice samples)

– Storage location: S3-compatible object storage in EU data centres — Hetzner Object Storage (Germany) and Scaleway Object Storage (France); processing in EU data centres (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

– Speicherort: Supabase (verwaltete Postgres-Datenbank, EU-Region); siehe Anlage 2 B.

– Aufbewahrungsdauer: Entsprechend deutschen Aufbewahrungsfristen (6-10 Jahre für Geschäftsunterlagen, je nach Art).

– Anonymisierung: Nach Aufbewahrungsfrist werden personenbezogene Daten anonymisiert oder gelöscht.

– Encryption: Encrypted on disk (encryption at rest).

– Access control: Only the organisation owner and authorised keys can retrieve samples.

– Deletion: Voice references are deleted on Customer request or after contract end.

4.3 Billing and metadata

– Storage location: Supabase (managed Postgres database, EU region); see Annex 2 B.

– Retention: In accordance with German statutory retention periods (6-10 years for business records, depending on type).

– Anonymisation: After the retention period, personal data is anonymised or deleted.

---

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: Kein 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.

5. DATA PROTECTION BY DESIGN AND BY DEFAULT

5.1 Privacy by design

– Data minimisation: Only the minimum necessary data is processed.

– Pseudonymisation: User IDs are represented internally by hashes; real user identities are not linked to request data.

– Data economy: No data sales, no secondary use without explicit consent.

5.2 Privacy policy & transparency

– KugelAudio provides clear documentation on data processing (see customer documentation).

– Every customer can see which data is stored and for which periods.

---

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.

6. SECURITY UPDATES AND PATCHING

– Updates: Security-relevant patches are applied promptly after availability and successful internal review.

– Critical vulnerabilities: Critical security vulnerabilities are prioritised and closed as quickly as possible.

– Maintenance windows: Necessary maintenance is performed outside core business hours where possible.

---

7. INCIDENT RESPONSE & FORENSIK

– 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.

7. INCIDENT RESPONSE & FORENSICS

– Incident management: A defined process exists for reporting and handling security incidents.

– Response times: Security incidents are responded to within the service hours agreed in the Main Agreement (SLA).

– Analysis: After a critical incident is resolved, an analysis is performed to prevent future risks.

---

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.

8. EXTERNAL AUDITS & CERTIFICATIONS

– Internal audits: KugelAudio performs regular (at least annual) internal security reviews of the technical measures.

– External certification: Certification against international industry standards (e.g. SOC 2 Type II or ISO 27001) is targeted and part of the long-term security roadmap. These certificates are not yet available at this time.

– Transparency: On request, KugelAudio provides the Customer with the results of internal security reviews (in summarised form).

ANLAGE 2: UNTERAUFTRAGSVERARBEITER (SUB-PROCESSORS)

ANNEX 2: SUB-PROCESSORS

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

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

KugelAudio kann Speech-Core-Workloads nach eigenem Ermessen aus Kapazitäts-, Resilienz-, Performance- oder Kostengründen zwischen den in dieser Anlage 2 A gelisteten Infrastruktur-Anbietern verlagern, verteilen oder migrieren. Da sämtliche dieser Anbieter bereits offengelegte Subunternehmer im Sinne dieses Vertrags sind, stellt eine solche Verlagerung keine Hinzuziehung eines neuen Subunternehmers dar und löst keine erneute Ankündigungsfrist nach § 6 aus.

A) CORE INFRASTRUCTURE (processing of audio & text data)

These providers have direct contact with the speech processing data (texts, audio, voice samples).

KugelAudio may route, balance or migrate Speech-Core workloads between the infrastructure providers listed in this Annex 2 A at its discretion for capacity, resilience, performance or cost reasons. Because all of these providers are already disclosed sub-processors under this agreement, such routing does not constitute the engagement of a new sub-processor and does not trigger a fresh notice period under § 6.

Dienstleister / Provider	Sitz / Location	Leistung / Service	Verarbeitungsort / Processing location	Rechtsgrundlage / Legal basis

Verda AI (GPU Cloud)	EU (Finnland / Finland)	GPU-Inferenz für TTS/STT-Modelle, Hosting / GPU inference for TTS/STT models, hosting	EU; vertraglich zugesichert / EU; contractually pinned	AVV (Data Processing Terms)
Hetzner Online GmbH	Deutschland (Gunzenhausen) / Germany	GPU-Server und Infrastruktur für KI-Modelle; S3-kompatibler Object Storage für Voice References / GPU servers and infrastructure for AI models; S3-compatible object storage for voice references	Deutschland (EU) / Germany (EU)	Subvertrag mit Datenschutzverpflichtung / Sub-contract with data protection obligations
Nebius B.V.	Niederlande / Netherlands	GPU-Cloud-Kapazität für TTS/STT-Inferenz und Modellbetrieb / GPU cloud capacity for TTS/STT inference and model operations	EU (u. a. Finnland, Frankreich) / EU (incl. Finland, France); EU-Regionen vertraglich festgelegt / EU regions contractually pinned	AVV/DPA des Anbieters (Art. 28 DSGVO) / provider DPA (Art. 28 GDPR)
Contabo GmbH	Deutschland (München) / Germany (Munich)	GPU-/Server-Infrastruktur / GPU and server infrastructure	Deutschland, EU / Germany, EU; EU-Regionen vertraglich festgelegt / EU regions contractually pinned	AVV/DPA des Anbieters (Art. 28 DSGVO) / provider DPA (Art. 28 GDPR)
OVH SAS (OVHcloud)	Frankreich (Roubaix) / France	GPU-/Server-Infrastruktur / GPU and server infrastructure	EU (Frankreich, Deutschland) / EU (France, Germany); EU-Regionen vertraglich festgelegt / EU regions contractually pinned	AVV/DPA des Anbieters (Art. 28 DSGVO) / provider DPA (Art. 28 GDPR)
Scaleway SAS	Frankreich (Paris) / France	GPU-/Server-Infrastruktur; S3-kompatibler Object Storage für Voice References / GPU and server infrastructure; S3-compatible object storage for voice references	EU (Frankreich, Niederlande, Polen) / EU (France, Netherlands, Poland); EU-Regionen vertraglich festgelegt / EU regions contractually pinned	AVV/DPA des Anbieters (Art. 28 DSGVO) / provider DPA (Art. 28 GDPR)

B) BUSINESS- & SUPPORT-INFRASTRUKTUR

Diese Dienstleister verarbeiten Business- bzw. Betriebsdaten (z. B. Account- und Abrechnungsdaten), haben aber KEINEN Zugriff auf Audio-/Text-Inhalte oder Voice Samples.

B) BUSINESS & SUPPORT INFRASTRUCTURE

These providers process business or operational data (e.g. account and billing data), but have NO access to audio/text content or voice samples.

Dienstleister / Provider	**Sitz / Location**	**Leistung / Service**	**Verarbeitungsort / Processing location**	**Rechtsgrundlage / Legal basis**	**Datenfluss / Data flow**
Supabase Pte. Ltd.	Singapur / Singapore	Verwaltete Postgres-Datenbank und Authentifizierung für Account- und Abrechnungsdaten / Managed Postgres database and authentication for account and billing data	EU-Region / EU region; EU-Regionen vertraglich festgelegt / EU regions contractually pinned	Supabase DPA + EU-Standardvertragsklauseln (SCC, Durchführungsbeschluss (EU) 2021/914) / Supabase DPA + EU Standard Contractual Clauses (SCCs, Implementing Decision (EU) 2021/914)	Account- und Abrechnungsdaten (E-Mail, Name, Organisation, Nutzungszähler); keine Audio-/Text-Inhalte und keine Voice References / Account and billing data (email, name, organisation, usage counters); no audio/text content and no voice references

Autoritatives DNS (kein Auftragsverarbeiter)

Die autoritative Namensauflösung der KugelAudio-Domains

Authoritative DNS (not a processor)

Authoritative name resolution for the KugelAudio domains,

einschließlich des DNS-basierten Geo-Steerings (Auflösung auf den jeweiligen Cluster-Endpunkt) erfolgt über einen externen Anycast-DNS-Anbieter. Dieser verarbeitet ausschließlich DNS-Auflösungsanfragen (Hostname und IP-Adresse des anfragenden Resolvers) und keine Inhalts-, Voice- oder Business-Daten im Auftrag von KugelAudio. Es findet KEINE TLS-Terminierung und KEIN CDN-/Reverse-Proxy-Transit statt: die Verbindung des Nutzers läuft direkt zur KugelAudio-Ingress-Infrastruktur. Der DNS-Anbieter wird daher nicht als Unterauftragsverarbeiter nach Art. 28 Abs. 4 DSGVO geführt und ist nicht in den vorstehenden Tabellen aufgeführt.

Error- und Performance-Monitoring (kein Auftragsverarbeiter)

Das Error- und Performance-Monitoring erfolgt auf einer von KugelAudio selbst betriebenen Installation (Self-Hosted Sentry). Sie läuft auf der in Anlage 2 A aufgeführten Infrastruktur in Deutschland; Error-Ereignisse werden ausschließlich an diese Installation übermittelt. Der Hersteller der Monitoring-Software (Functional Software, Inc.) erhält hierbei keine Daten im Auftrag von KugelAudio und wird daher nicht als Unterauftragsverarbeiter nach Art. 28 Abs. 4 DSGVO geführt. Verarbeitet werden weiterhin ausschließlich technische Error-Logs, keine Audio-/Text-Payloads und keine Voice References.

including DNS-based geo-steering (resolution to the respective cluster endpoint), is provided by an external anycast DNS provider. That provider processes DNS resolution queries only (hostname and IP address of the requesting resolver) and no content, voice or business data on KugelAudio's behalf. There is NO TLS termination and NO CDN or reverse-proxy transit: the user's connection goes directly to KugelAudio's ingress infrastructure. The DNS provider is therefore not carried as a sub-processor within the meaning of Art. 28(4) GDPR and is not listed in the tables above.

Error and performance monitoring (not a processor)

Error and performance monitoring runs on an installation operated by KugelAudio itself (self-hosted Sentry). It runs on the infrastructure listed in Annex 2 A in Germany, and error events are transmitted to that installation only. The vendor of the monitoring software (Functional Software, Inc.) receives no data on KugelAudio's behalf in this arrangement and is therefore not carried as a sub-processor within the meaning of Art. 28(4) GDPR. As before, only technical error logs are processed: no audio/text payloads and no voice references.

ERKLÄRUNGEN ZU DATENFLÜSSEN

Audio- und Text-Sicherheit

Input-Texte und generiertes Audio werden ausschließlich in der EU verarbeitet und gespeichert. Die TLS-Verbindung des Nutzers wird direkt auf der KugelAudio-Ingress-Infrastruktur in der EU terminiert; ein TLS-terminierender CDN- oder Reverse-Proxy-Dienst wird nicht eingesetzt. Der externe DNS-Anbieter (siehe Anlage 2 B) löst lediglich den Namen auf den EU-Cluster-Endpunkt auf; Inhalte werden nicht über ihn geleitet. Audio-/Text-Inhalte kommen nicht in Kontakt mit US-Verarbeitungsstandorten.

```
DNS-Auflösung (externer DNS-Anbieter) — nur
Namensauflösung, kein Inhaltstransit
  ↓
Nutzer-Input (Text/Audio)
  ↓
HTTPS/WSS (TLS) → KugelAudio-Ingress (EU) ← TLS-
Terminierung findet HIER statt
  ↓
EU-GPU-Cloud (Anbieter siehe Anlage 2 A) ← TTS-
Verarbeitung findet HIER statt
  ↓
Audio-Stream → Nutzer via WSS
  ↓
[Audio wird nicht gespeichert oder an Dritte
weitergegeben]
[Voice References (optional): S3-Object-Storage in der
EU — Hetzner (Deutschland) / Scaleway (Frankreich),
verschlüsselt at Rest]
```

Business-Daten (EU-Only Hosting)

DATA FLOW EXPLANATIONS

Audio and text security

Input texts and generated audio are processed and stored exclusively in the EU. The user's TLS connection is terminated directly on KugelAudio's ingress infrastructure in the EU; no TLS-terminating CDN or reverse-proxy service is used. The external DNS provider (see Annex 2 B) only resolves the name to the EU cluster endpoint; content is not routed through it. Audio/text content does not come into contact with US processing locations.

```
DNS resolution (external DNS provider) — name
resolution only, no content transit
  ↓
User input (text/audio)
  ↓
HTTPS/WSS (TLS) → KugelAudio ingress (EU) ← TLS
termination happens HERE
  ↓
EU GPU cloud (providers per Annex 2 A) ← TTS
processing happens HERE
  ↓
Audio stream → user via WSS
  ↓
[Audio is not stored or shared with third parties]
[Voice references (optional): S3 object storage in the
EU — Hetzner (Germany) / Scaleway (France), encrypted
at rest]
```

Business data (EU-only hosting)

```
Kunde registriert sich
  ↓
E-Mail, Name, Abrechnungsdaten → Supabase (verwaltete
Postgres-Datenbank, EU-Region)
  ↓
Error-Logs → Self-Hosted Monitoring auf KugelAudio-
Infrastruktur (Deutschland)
  ↓
[Zahlungsdaten werden direkt vom Zahlungsanbieter
(eigener Verantwortlicher) verarbeitet und berühren
diesen AVV nicht]
```

Internationales Datenschutzniveau

Alle Verarbeitungsregionen sind auf die EU festgelegt. In dieser Variante wird kein Unterauftragsverarbeiter mit Sitz oder Muttergesellschaft in den USA eingesetzt. Für einen etwaigen verbleibenden Drittlandzugriff durch den einzigen außerhalb der EU ansässigen Unterauftragsverarbeiter (Supabase Pte. Ltd., Singapur) gelten gemäß Art. 46 DSGVO die EU-Standardvertragsklauseln (SCC), ergänzt durch: Encryption at Rest / in Transit, strikte Zugriffskontrolle (nur KugelAudio-Mitarbeiter), keine Weitergabe an Behörden ohne Benachrichtigung.

```
Customer signs up
  ↓
Email, name, billing data → Supabase (managed Postgres
database, EU region)
  ↓
Error logs → self-hosted monitoring on KugelAudio
infrastructure (Germany)
  ↓
[Payment data is processed directly by the payment
provider (independent controller) and is not covered
by this DPA]
```

International data protection level

All processing regions are pinned to the EU. No sub-processor established in, or with a parent company in, the USA is engaged under this variant. For any residual third-country access by the only sub-processor established outside the EU (Supabase Pte. Ltd., Singapore), EU Standard Contractual Clauses (SCCs) apply pursuant to Art. 46 GDPR, supplemented by: encryption at rest / in transit, strict access control (KugelAudio employees only), no disclosure to authorities without notification.

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.

CHANGES TO THE LIST

The process for engaging or replacing sub-processors (including notification obligations and objection periods) is governed by § 6 of this agreement.

„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: 19.08.2026 (Version 2026-08-19)

"This agreement is concluded electronically and is valid without a handwritten signature. By accepting the Terms of Service or by using the platform, this agreement is deemed concluded."

As of: 19.08.2026 (version 2026-08-19)