Auftragsverarbeitungsvertrag (AVV)

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Version 2.1 · Produkt: DigitalTwin Plattform · Stand: Juni 2026

VERANTWORTLICHER

Der Kunde als Vertragspartner des Hauptvertrags
– nachfolgend „Verantwortlicher“ –

AUFTRAGSVERARBEITER

Ankerkern
Warthestr. 48
12051 Berlin, Deutschland
– nachfolgend „Auftragsverarbeiter“ –

– gemeinsam die „Parteien“ –

§ 1 Gegenstand, Geltung und Dauer des Auftrags

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die SaaS-Plattform „DigitalTwin“ zur Digitalisierung und Automatisierung von Geschäftsprozessen bereit (einschließlich Kundenkommunikation, Sprachaufnahme, E-Mail- und Dokumenten-Workflows sowie ERP-Unterstützung). Gegenstand dieses Vertrags ist die dabei erfolgende Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen. Einzelheiten ergeben sich aus dem zugrunde liegenden Hauptvertrag und aus Anlage 1.

(2) Dieser Vertrag wird automatisch mit Abschluss des Hauptvertrags, spätestens jedoch mit der ersten Nutzung der Plattform durch den Verantwortlichen, wirksam. Einer gesonderten Unterschrift der Parteien bedarf es nicht. Auf Wunsch des Verantwortlichen stellt der Auftragsverarbeiter eine unterzeichnete Fassung bereit.

(3) Die Dauer dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet automatisch mit dessen Beendigung; die Pflichten aus § 11 (Löschung und Rückgabe) gelten darüber hinaus fort.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck der Verarbeitung ergeben sich abschließend aus Anlage 1. Die Verarbeitung umfasst insbesondere das Erheben, Speichern, Strukturieren, Auswerten (einschließlich KI-gestützter Verarbeitung), Übermitteln und Löschen personenbezogener Daten im Rahmen der Plattformnutzung.

(2) Die Verarbeitung findet grundsätzlich in der Europäischen Union statt (Rechenzentrum: IONOS, Frankfurt am Main). Übermittlungen in Drittländer richten sich nach § 9.

§ 3 Kategorien betroffener Personen und Datenkategorien

(1) Die Kategorien betroffener Personen und die verarbeiteten Datenkategorien sind in Anlage 1 festgelegt.

(2) Die Plattform ist bestimmungsgemäß nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. Gesundheitsdaten) oder von Gehalts- und Lohnabrechnungsdaten ausgelegt. Der Verantwortliche stellt sicher, dass solche Daten nicht zur Verarbeitung übergeben werden.

§ 4 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation –, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen

Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Der Hauptvertrag, dieser Vertrag und die Nutzung der vereinbarten Plattformfunktionen gelten als dokumentierte Weisung. Ergänzende Einzelweisungen bedürfen der Textform (z. B. E-Mail). Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er 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). Er ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

§ 5 Pflichten des Auftragsverarbeiters

(1) Vertraulichkeit: Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Vertraulichkeitspflicht besteht auch nach Beendigung der Tätigkeit fort.

(2) Sicherheit der Verarbeitung: Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM). Die zum Zeitpunkt des Vertragsschlusses umgesetzten Maßnahmen sind in Anlage 3 bzw. dem dort referenzierten TOM-Dokument beschrieben. Der Auftragsverarbeiter darf die Maßnahmen an den Stand der Technik anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen werden dokumentiert.

(3) Beauftragte Personen: Nur solche Beschäftigte und sonstige Erfüllungsgehilfen erhalten Zugang zu personenbezogenen Daten, die diesen für die Erfüllung ihrer Aufgaben benötigen (Need-to-know-Prinzip, Art. 29, Art. 32 Abs. 4 DSGVO).

(4) Ansprechpartner für Datenschutz: Der Auftragsverarbeiter benennt dem Verantwortlichen einen Ansprechpartner für alle datenschutzrechtlichen Fragen im Rahmen dieses Vertrags: Dr. Andreas Engler, E-Mail: datenschutz@ankerkern.de. Soweit eine gesetzliche Pflicht zur Benennung eines Datenschutzbeauftragten besteht, kommt der Auftragsverarbeiter dieser nach.

(5) Verzeichnis von Verarbeitungstätigkeiten: Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

(6) Zusammenarbeit mit Aufsichtsbehörden: Der Auftragsverarbeiter arbeitet auf Anfrage mit der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen und informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie diesen Auftrag betreffen.

§ 6 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die im Rahmen dieses Auftrags verarbeitet werden, unverzüglich nach Bekanntwerden (Art. 33 Abs. 2 DSGVO).

(2) Die Meldung enthält, soweit bekannt, mindestens: (a) eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze, (b) Name und Kontaktdaten des Ansprechpartners, (c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung, (d) eine Beschreibung der ergriffenen oder vorgeschlagenen Abhilfemaßnahmen. Informationen können schrittweise nachgereicht werden, soweit sie nicht sofort verfügbar sind.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Melde- und Benachrichtigungspflichten gemäß Art. 33 und 34 DSGVO und ergreift unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

§ 7 Unterstützungspflichten

(1) Betroffenenrechte: Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte gemäß Kapitel III DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter. Der Auftragsverarbeiter erteilt betroffenen Personen keine Auskünfte ohne vorherige Weisung des Verantwortlichen.

(3) Datenschutz-Folgenabschätzung: Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde (Art. 28 Abs. 3 lit. f DSGVO).

(4) Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind und über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen, kann der Auftragsverarbeiter eine angemessene Vergütung auf Grundlage der vereinbarten Stundensätze verlangen.

§ 8 Unterauftragsverhältnisse (Subunternehmer)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Einschaltung weiterer Auftragsverarbeiter (Subunternehmer) im Sinne von Art. 28 Abs. 2 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmer sind in Anlage 2 aufgeführt und gelten als genehmigt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Subunternehmers mindestens vier Wochen im Voraus in Textform (z. B. per E-Mail an den benannten Ansprechpartner des Verantwortlichen).

(3) Der Verantwortliche kann der Änderung innerhalb von zwei Wochen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Im Fall eines Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung; gelingt dies nicht, ist jede Partei berechtigt, den Hauptvertrag mit angemessener Frist außerordentlich zu kündigen.

(4) Der Auftragsverarbeiter erlegt jedem Subunternehmer im Wege eines Vertrags dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmers.

(5) Nicht als Unterauftragsverhältnisse gelten Nebenleistungen ohne unmittelbaren Bezug zur Auftragsverarbeitung (z. B. Post- und Kurierdienste, Reinigungs- und Wachdienste, Wartungsleistungen ohne Datenzugriff).

§ 9 Übermittlungen in Drittländer

(1) Die Verarbeitung erfolgt grundsätzlich in der Europäischen Union. Eine Übermittlung personenbezogener Daten in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission (einschließlich des EU-US Data Privacy Framework, DPF) oder der EU-Standardvertragsklauseln (SCCs) nebst erforderlicher ergänzender Maßnahmen.

(2) Die für jeden Subunternehmer einschlägigen Übermittlungsgarantien sind in Anlage 2 ausgewiesen.

§ 10 Nachweis- und Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis kann insbesondere erfolgen durch: (a) aktuelle Testate oder Zertifizierungen (z. B. ISO 27001 des Rechenzentrumsbetreibers), (b) Berichte unabhängiger Prüfer, (c) Selbstauskünfte und die Dokumentation der TOM, (d) genehmigte Verhaltensregeln oder Zertifizierungen nach Art. 40, 42 DSGVO.

(3) Soweit im Einzelfall darüber hinaus Inspektionen vor Ort erforderlich sind, ermöglicht der Auftragsverarbeiter diese während der üblichen Geschäftszeiten nach vorheriger Anmeldung mit angemessener Frist (in der Regel 14 Kalendertage) und ohne Störung des Betriebsablaufs – im Regelfall höchstens einmal pro Kalenderjahr, bei konkretem Anlass (z. B. Datenschutzvorfall) auch darüber hinaus.

(4) Der Verantwortliche kann Kontrollen durch beauftragte Dritte durchführen lassen, sofern diese nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen und einer Verschwiegenheitspflicht unterliegen. Jede Partei trägt die ihr durch die Kontrolle entstehenden Kosten; bei Kontrollen aufgrund eines vom Auftragsverarbeiter zu vertretenden Anlasses trägt dieser die angemessenen Kosten.

§ 11 Löschung und Rückgabe personenbezogener Daten

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen oder gibt sie zurück (Art. 28 Abs. 3 lit. g DSGVO). Die Rückgabe erfolgt in einem gängigen, strukturierten Format (z. B. Datenbank-Export des Mandanten-Schemas und Export der Objektspeicher-Inhalte).

(2) Übt der Verantwortliche sein Wahlrecht nicht innerhalb von 30 Tagen nach Vertragsende aus, gilt Löschung als gewählt. Während dieser 30-tägigen Übergangsfrist ist der Mandant (Tenant) gesperrt; eine aktive Verarbeitung findet nicht statt. Anschließend erfolgt die vollständige Löschung aller Mandanten-Datenbankschemata, Objektspeicher-Buckets und Container-Volumes innerhalb von 7 Tagen.

(3) Backups: Datensicherungen werden rollierend überschrieben (tägliche Sicherungen: 7 Tage Vorhaltung; wöchentliche Sicherungen: 12 Wochen Vorhaltung). Personenbezogene Daten in Backups sind damit spätestens 12 Wochen nach der Löschung gemäß Absatz 2 vollständig entfernt. Bis dahin sind die Backups gegen Zugriff gesichert und werden nicht aktiv verarbeitet; eine Wiederherstellung erfolgt nur zur Erfüllung gesetzlicher Pflichten oder auf Weisung des Verantwortlichen.

(4) KI-Verarbeitungsprotokolle: Protokolle KI-gestützter Verarbeitungsvorgänge (Prompt-Sessions) werden während der Vertragslaufzeit für längstens 24 Monate rollierend gespeichert, um dem Verantwortlichen die Nachvollziehbarkeit automatisierter Verarbeitungen zu ermöglichen. Bei Vertragsende werden sie nach Maßgabe der Absätze 1 bis 3 gelöscht bzw. zurückgegeben.

(5) Konfigurationsvorlagen des Auftragsverarbeiters (z. B. Prompt-Templates) ohne personenbezogene Daten verbleiben als Geschäftsgeheimnis beim Auftragsverarbeiter.

(6) Gesetzliche Aufbewahrungspflichten bleiben unberührt; betroffene Daten werden für die Dauer der Aufbewahrungspflicht in der Verarbeitung eingeschränkt und anschließend gelöscht.

(7) Auf Verlangen bestätigt der Auftragsverarbeiter die vollständige Löschung in Textform.

§ 12 Haftung

(1) Für die Haftung der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten gilt Art. 82 DSGVO.

(2) Im Innenverhältnis haften die Parteien einander entsprechend ihrem jeweiligen Verursachungs- und Verschuldensbeitrag. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Dies gilt auch für die Änderung dieser Klausel.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich des Datenschutzes die Regelungen dieses Vertrags vor.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand ist – soweit gesetzlich zulässig – der Sitz des Auftragsverarbeiters.

(4) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die dem wirtschaftlich und datenschutzrechtlich Gewollten am nächsten kommt.

(5) Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags.

(6) Nur die deutsche Fassung dieses Vertrags ist rechtlich bindend. Die englische Übersetzung dient ausschließlich Informationszwecken.

ANLAGE 1

Gegenstand der Verarbeitung, Datenkategorien, betroffene Personen

1. Gegenstand, Art und Zweck der Verarbeitung

Der Auftragsverarbeiter betreibt eine mandantenfähige SaaS-Plattform („DigitalTwin“), gehostet auf IONOS-Infrastruktur in Frankfurt am Main. Die Verarbeitung umfasst:

- Backend- und Frontend-Betrieb zur Abbildung und Automatisierung von Geschäftsprozessen,
- Mandantentrennung über separate Datenbankschemata und mandantenspezifische Objektspeicher-Buckets,
- selbst gehostete Sprach- und Telefonieprozesse (SIP-Trunks durch Easybell),
- KI-gestützte Verarbeitung über externe Sprachmodelle (LLMs) oder selbst gehostete Modelldienste, jeweils mit vertraglich vereinbartem Ausschluss der Nutzung von Kundendaten zu Trainingszwecken.

2. Kategorien personenbezogener Daten

Kategorie	Beispiele
Geschäftsprozessdaten	Finanz- und Buchhaltungsdaten, Projektdaten, Bestands-, Waren- und Fuhrparkdaten
Kommunikationsdaten	E-Mails, Chat-Nachrichten, Sprachaufnahmen (Voice Intake), Transkripte, Zusammenfassungen
Stammdaten	Namen, Funktionen/Rollen, Kundennummern, interne Referenzen
Technische Daten	IP-Adressen, Audit-Logs, Authentifizierungs-Token, Systemereignisse

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie Gehalts- und Lohnabrechnungsdaten sind von der Verarbeitung bestimmungsgemäß ausgeschlossen (§ 3 Abs. 2 des Vertrags).

3. Kategorien betroffener Personen

- Beschäftigte und Administratoren des Verantwortlichen,
- Kunden und Interessenten des Verantwortlichen,
- Lieferanten und Geschäftspartner des Verantwortlichen,
- sonstige Kommunikationspartner, die in die automatisierten Workflows einbezogen sind.

ANLAGE 2

Genehmigte Subunternehmer

Stand: Juni 2026. Über Änderungen wird gemäß § 8 des Vertrags informiert.

Subunternehmer	Zweck	Ort der Verarbeitung	Übermittlungsgarantie
IONOS SE	Cloud-Infrastruktur, Speicher, Datenbanken, Backup	Frankfurt a. M., Deutschland	EU – keine Drittlandübermittlung (ISO 27001 zertifiziert)
Easybell GmbH	Telefonie / SIP-Trunking	Berlin, Deutschland	EU – keine Drittlandübermittlung
OpenAI	LLM-Verarbeitung (Trainings-Opt-out)	EU-Datenresidenz	EU-US DPF und SCCs für etwaige Zugriffe aus den USA (z. B. Support)
Anthropic	LLM-Verarbeitung (Trainings-Opt-out)	EU-Region / USA	EU-US DPF und SCCs
Google Cloud (GCP)	Transkription, LLM-Fallback (Trainings-Opt-out)	EU-Region	EU-US DPF und SCCs für etwaige Zugriffe aus den USA
Deepgram Inc.	Speech-to-Text	EU-Region / USA	SCCs
Cartesia AI Inc.	Text-to-Speech	EU-Region / USA	SCCs
Twilio Inc.	SMS- und WhatsApp-Routing	EU-Hosting / USA	EU-US DPF und SCCs

Bei allen eingesetzten KI-Diensten ist die Nutzung von Kundendaten zum Training der Modelle vertraglich ausgeschlossen („Zero Data Retention“ bzw. Trainings-Opt-out). Die jeweils aktuelle Subunternehmer-Liste ist im Trust Center unter ankerkern.de/sicherheit einsehbar.

ANLAGE 3

Technische und organisatorische Maßnahmen (TOM)

Die vollständigen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind im separaten Dokument „Ankerkern TOM“ (jeweils aktuelle Version) beschrieben, das als Bestandteil dieser Anlage gilt. Die Kernmaßnahmen im Überblick:

Maßnahmenbereich	Umsetzung (Auszug)
Verschlüsselung (Art. 32 Abs. 1 lit. a)	AES-256-Verschlüsselung ruhender Daten (Datenbanken, Volumes); Transportverschlüsselung TLS 1.2 oder höher für alle Verbindungen
Vertraulichkeit (Art. 32 Abs. 1 lit. b)	Logische Mandantentrennung auf Schema-Ebene und über mandantenspezifische Objektspeicher-Buckets; rollenbasierte Zugriffskontrolle; Need-to-know-Prinzip; Authentifizierung mit Token-Verfahren
Integrität (Art. 32 Abs. 1 lit. b)	Audit-Logging sicherheitsrelevanter Ereignisse; Protokollierung von Systemzugriffen und Änderungen
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c)	Tägliche Backups (7 Tage Vorhaltung), wöchentliche Backups (12 Wochen Vorhaltung); Betrieb in ISO-27001-zertifiziertem Rechenzentrum (IONOS, Frankfurt)
Regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d)	Regelmäßige Überprüfung und Anpassung der TOM an den Stand der Technik; Dokumentation wesentlicher Änderungen

Das vollständige TOM-Dokument ist im Trust Center unter ankerkern.de/sicherheit abrufbar und wird dem Verantwortlichen auf Anfrage in der jeweils aktuellen Fassung bereitgestellt.

ENGLISH VERSION

Non-binding translation · Only the German version is legally binding (§ 13(6))

ankerkern

TRUST & COMPLIANCE

Data Processing Agreement (DPA)

Agreement for the processing of personal data on behalf of a controller pursuant to Art. 28 General Data Protection Regulation (GDPR)

Version 2.1 · Product: DigitalTwin Platform · As of: June 2026

CONTROLLER

The customer as party to the main contract
– hereinafter the “Controller” –

PROCESSOR

Ankerkern
Warthestr. 48
12051 Berlin, Germany
– hereinafter the “Processor” –

– together the “Parties” –

§ 1 Subject Matter, Applicability and Duration

(1) The Processor provides the Controller with the “DigitalTwin” SaaS platform for digitizing and automating business processes (including customer communication, voice intake, email and document workflows, and ERP support). The subject matter of this Agreement is the processing of personal data on behalf of the Controller in this context. Details follow from the underlying main contract and from Annex 1.

(2) This Agreement takes effect automatically upon conclusion of the main contract and, at the latest, upon the Controller’s first use of the platform. No separate signature by the Parties is required. Upon the Controller’s request, the Processor will provide a signed copy.

(3) The duration of this Agreement corresponds to the term of the main contract. It ends automatically upon its termination; the obligations under § 11 (deletion and return) survive termination.

§ 2 Nature, Purpose and Scope of Processing

(1) The nature and purpose of the processing are set out conclusively in Annex 1. Processing includes in particular the collection, storage, structuring, analysis (including AI-assisted processing), transmission and deletion of personal data in the course of platform use.

(2) Processing takes place in the European Union as a rule (data center: IONOS, Frankfurt am Main, Germany). Transfers to third countries are governed by § 9.

§ 3 Categories of Data Subjects and Data Categories

(1) The categories of data subjects and the categories of personal data processed are specified in Annex 1.

(2) The platform is by design not intended for the processing of special categories of personal data within the meaning of Art. 9 GDPR (e.g. health data) or of payroll and salary data. The Controller shall ensure that no such data is submitted for processing.

§ 4 Right of Instruction of the Controller

(1) The Processor processes personal data only on documented instructions from the Controller — including with regard to transfers of personal data to a third country or an international organisation — unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28(3)(a) GDPR).

(2) The main contract, this Agreement and the use of the agreed platform functions constitute documented instructions. Additional individual instructions must be given in text form (e.g. email). Instructions given orally shall be confirmed in text form without undue delay.

(3) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions (Art. 28(3) sentence 3 GDPR). The Processor is entitled to suspend the execution of the instruction concerned until it is confirmed or amended by the Controller.

§ 5 Obligations of the Processor

(1) Confidentiality: The Processor ensures that the persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR). The duty of confidentiality continues to apply after the end of their engagement.

(2) Security of processing: The Processor implements all technical and organisational measures (TOMs) required pursuant to Art. 32 GDPR. The measures implemented at the time of conclusion of this Agreement are described in Annex 3 and the TOMs document referenced therein. The Processor may adapt the measures to the state of the art, provided that the agreed level of protection is not reduced; material changes will be documented.

(3) Authorised persons: Only those employees and other agents who require access to personal data for the performance of their tasks are granted such access (need-to-know principle, Art. 29, Art. 32(4) GDPR).

(4) Data protection contact: The Processor designates a contact person for all data protection matters under this Agreement: Dr. Andreas Engler, email: datenschutz@ankerkern.de. Where a statutory obligation to appoint a data protection officer exists, the Processor will comply with it.

(5) Records of processing activities: The Processor maintains records of all categories of processing activities carried out on behalf of the Controller in accordance with Art. 30(2) GDPR.

(6) Cooperation with supervisory authorities: The Processor cooperates, on request, with the competent supervisory authority in the performance of its tasks and informs the Controller without undue delay of any inspections or measures by the supervisory authority insofar as they relate to this engagement.

§ 6 Notification of Personal Data Breaches

(1) The Processor notifies the Controller of any personal data breach concerning data processed under this engagement without undue delay after becoming aware of it (Art. 33(2) GDPR).

(2) The notification shall contain, as far as known: (a) a description of the nature of the breach including, where possible, the categories and approximate number of data subjects and records concerned, (b) the name and contact details of the contact person, (c) a description of the likely consequences of the breach, (d) a description of the measures taken or proposed to address the breach. Information may be provided in phases where it is not immediately available.

(3) The Processor supports the Controller in fulfilling its notification and communication obligations under Art. 33 and 34 GDPR and takes appropriate measures without undue delay to secure the data and mitigate possible adverse effects.

§ 7 Assistance Obligations

(1) Data subject rights: Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests for exercising data subject rights under Chapter III GDPR (access, rectification, erasure, restriction, data portability, objection) (Art. 28(3)(e) GDPR).

(2) If a data subject contacts the Processor directly, the Processor forwards the request to the Controller without undue delay. The Processor does not provide information to data subjects without prior instruction from the Controller.

(3) Data protection impact assessment: The Processor assists the Controller, taking into account the nature of processing and the information available to it, in ensuring compliance with the obligations pursuant to Art. 32 to 36 GDPR, in particular data protection impact assessments and prior consultations of the supervisory authority (Art. 28(3)(f) GDPR).

(4) For assistance not attributable to a fault of the Processor and exceeding the scope of services agreed in the main contract, the Processor may charge reasonable remuneration based on the agreed hourly rates.

§ 8 Sub-processors

(1) The Controller grants the Processor general authorisation to engage further processors (sub-processors) within the meaning of Art. 28(2) GDPR. The sub-processors engaged at the time of conclusion of this Agreement are listed in Annex 2 and are deemed approved.

(2) The Processor informs the Controller of any intended addition or replacement of a sub-processor at least four weeks in advance in text form (e.g. by email to the Controller's designated contact).

(3) The Controller may object to the change within two weeks of receipt of the information on important data protection grounds. If no objection is raised, the change is deemed approved. In the event of an objection, the Parties shall endeavour to find an amicable solution; if this fails, either Party is entitled to terminate the main contract extraordinarily with reasonable notice.

(4) The Processor imposes on each sub-processor, by way of contract, the same data protection obligations as set out in this Agreement, in particular sufficient guarantees to implement appropriate technical and organisational measures (Art. 28(4) GDPR). Where a sub-processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of that sub-processor's obligations.

(5) Ancillary services without a direct relation to the processing (e.g. postal and courier services, cleaning and security services, maintenance without data access) do not constitute sub-processing.

§ 9 Transfers to Third Countries

(1) Processing takes place in the European Union as a rule. Personal data is transferred to a third country only if the requirements of Art. 44 et seq. GDPR are met, in particular on the basis of an adequacy decision of the EU Commission (including the EU-US Data Privacy Framework, DPF) or the EU Standard Contractual Clauses (SCCs) together with supplementary measures where required.

(2) The transfer safeguards applicable to each sub-processor are set out in Annex 2.

§ 10 Evidence and Audit Rights of the Controller

(1) The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR (Art. 28(3)(h) GDPR).

(2) Evidence may in particular be provided by: (a) current attestations or certifications (e.g. ISO 27001 of the data center operator), (b) reports by independent auditors, (c) self-assessments and the TOMs documentation, (d) approved codes of conduct or certifications pursuant to Art. 40, 42 GDPR.

(3) Where on-site inspections are additionally required in individual cases, the Processor enables them during regular business hours, upon prior notice with reasonable lead time (as a rule 14 calendar days) and without disrupting business operations — as a rule no more than once per calendar year, and additionally where there is a specific cause (e.g. a data breach).

(4) The Controller may have audits carried out by commissioned third parties, provided they are not competitors of the Processor and are bound by confidentiality. Each Party bears its own costs of an audit; in the case of audits prompted by a cause attributable to the Processor, the Processor bears the reasonable costs.

§ 11 Deletion and Return of Personal Data

(1) After completion of the processing services, the Processor deletes all personal data or returns it, at the choice of the Controller (Art. 28(3)(g) GDPR). Return takes place in a common, structured format (e.g. database export of the tenant schema and export of the object storage contents).

(2) If the Controller does not exercise its choice within 30 days of termination, deletion is deemed chosen. During this 30-day transition period the tenant is locked; no active processing takes place. Thereafter, all tenant database schemas, object storage buckets and container volumes are fully deleted within 7 days.

(3) Backups: Backups are overwritten on a rolling basis (daily backups: 7-day retention; weekly backups: 12-week retention). Personal data in backups is thus fully removed no later than 12 weeks after deletion pursuant to paragraph 2. Until then, backups are secured against access and are not actively processed; restoration takes place only to comply with statutory obligations or on the Controller's instruction.

(4) AI processing logs: Logs of AI-assisted processing operations (prompt sessions) are stored on a rolling basis for a maximum of 24 months during the contract term to enable the Controller to trace automated processing. Upon termination they are deleted or returned in accordance with paragraphs 1 to 3.

(5) Configuration templates of the Processor (e.g. prompt templates) that contain no personal data remain with the Processor as trade secrets.

(6) Statutory retention obligations remain unaffected; the data concerned is restricted from processing for the duration of the retention obligation and deleted thereafter.

(7) Upon request, the Processor confirms complete deletion in text form.

§ 12 Liability

(1) The liability of the Parties in connection with the processing of personal data is governed by Art. 82 GDPR.

(2) As between the Parties, each Party is liable in proportion to its respective contribution to the cause and its degree of fault. In all other respects, the liability provisions of the main contract apply.

§ 13 Final Provisions

(1) Amendments and supplements to this Agreement require text form. This also applies to any amendment of this clause.

(2) In the event of contradictions between this Agreement and the main contract, the provisions of this Agreement prevail with respect to data protection.

(3) This Agreement is governed by the laws of the Federal Republic of Germany. The exclusive place of jurisdiction is — to the extent legally permissible — the registered seat of the Processor.

(4) Should individual provisions of this Agreement be or become invalid, the validity of the remaining provisions remains unaffected. The invalid provision shall be replaced by a provision that comes closest to the commercial and data protection intent.

(5) Annexes 1 to 3 form an integral part of this Agreement.

(6) Only the German version of this Agreement is legally binding. The English translation is provided for information purposes only.

ANNEX 1

Subject Matter of Processing, Data Categories, Data Subjects

1. Subject Matter, Nature and Purpose of Processing

The Processor operates a multi-tenant SaaS platform ("DigitalTwin") hosted on IONOS infrastructure in Frankfurt am Main, Germany. Processing encompasses:

- backend and frontend operations for mapping and automating business processes,
- tenant separation via dedicated database schemas and tenant-specific object storage buckets,
- self-hosted voice and telephony processes (SIP trunks provided by Easybell),
- AI-assisted processing using external large language models (LLMs) or self-hosted model services, in each case with a contractually agreed exclusion of the use of customer data for training purposes.

2. Categories of Personal Data

Category	Examples
Business process data	Finance and accounting data, project details, inventory, goods and fleet management data
Communication data	Emails, chat messages, voice intake audio, transcripts, summaries
Master data	Names, company roles, client numbers, internal references
Technical data	IP addresses, audit logs, authentication tokens, system events

Special categories of personal data (Art. 9 GDPR) as well as payroll and salary data are excluded from processing by design (§ 3(2) of this Agreement).

3. Categories of Data Subjects

- employees and administrators of the Controller,
- customers and prospective clients of the Controller,
- suppliers and business partners of the Controller,
- other communication partners involved in the automated workflows.

ANNEX 2

Approved Sub-processors

As of June 2026. Changes are communicated in accordance with § 8 of this Agreement.

Sub-processor	Purpose	Processing location	Transfer safeguard
IONOS SE	Cloud infrastructure, storage, databases, backup	Frankfurt am Main, Germany	EU – no third-country transfer (ISO 27001 certified)
Easybell GmbH	Telephony / SIP trunking	Berlin, Germany	EU – no third-country transfer
OpenAI	LLM processing (training opt-out)	EU data residency	EU-US DPF and SCCs for any access from the USA (e.g. support)
Anthropic	LLM processing (training opt-out)	EU region / USA	EU-US DPF and SCCs
Google Cloud (GCP)	Transcription, LLM fallback (training opt-out)	EU region	EU-US DPF and SCCs for any access from the USA
Deepgram Inc.	Speech-to-Text	EU region / USA	SCCs
Cartesia AI Inc.	Text-to-Speech	EU region / USA	SCCs
Twilio Inc.	SMS and WhatsApp routing	EU hosting / USA	EU-US DPF and SCCs

For all AI services used, the use of customer data for model training is contractually excluded (“zero data retention” or training opt-out). The current sub-processor list is available in the Trust Center at ankerkern.de/sicherheit.

ANNEX 3

Technical and Organisational Measures (TOMs)

The complete technical and organisational measures pursuant to Art. 32 GDPR are described in the separate document “Ankerkern TOMs” (current version), which is deemed part of this Annex. Core measures at a glance:

Area	Implementation (excerpt)
Encryption (Art. 32(1)(a))	AES-256 encryption at rest (databases, volumes); transport encryption TLS 1.2 or higher for all connections
Confidentiality (Art. 32(1)(b))	Logical tenant separation at schema level and via tenant-specific object storage buckets; role-based access control; need-to-know principle; token-based authentication
Integrity (Art. 32(1)(b))	Audit logging of security-relevant events; logging of system access and changes
Availability and resilience (Art. 32(1)(b), (c))	Daily backups (7-day retention), weekly backups (12-week retention); operation in an ISO 27001 certified data center (IONOS, Frankfurt)
Regular review (Art. 32(1)(d))	Regular review and adaptation of the TOMs to the state of the art; documentation of material changes

The complete TOMs document is available in the Trust Center at ankerkern.de/sicherheit and is provided to the Controller in its current version upon request.