Auftragsverarbeitungsvertrag

mitteldeutsche-IT GmbH

Vereinbarung zur Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (EU-DSGVO)

Zwischen

Test für Laura

Teststraße 1
12345 Teststadt

– Auftraggeber –

und

mitteldeutsche-IT GmbH

Debyestraße 5b
04329 Leipzig

– Auftragnehmer –

Präambel

(1) Der Auftraggeber nutzt vom Auftragnehmer erbrachte IT-Dienstleistungen, insbesondere Cloud-Services (IaaS, PaaS, SaaS, „mIT Office“) sowie optional KI-bezogene Infrastruktur- und Plattformdienste („KI-Services“). Im Rahmen dieser Leistungen verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.
(2) Der Auftraggeber bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO für die Verarbeitung personenbezogener Daten. Der Auftragnehmer verarbeitet diese Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und im Einklang mit dieser Vereinbarung.
(3) Diese Vereinbarung konkretisiert die Rechte und Pflichten der Parteien gemäß Art. 28 DS-GVO im Zusammenhang mit der im zugrunde liegenden Hauptvertrag beschriebenen Auftragsverarbeitung.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit den im Hauptvertrag beschriebenen Leistungen (insbesondere Bereitstellung und Betrieb von Rechenzentrumsressourcen, Cloud-Services und KI-Services).
(2) Art, Umfang und Zweck der Datenverarbeitung sowie die Kategorien der verarbeiteten Daten und der betroffenen Personen ergeben sich aus § 2 dieser Vereinbarung sowie aus Anhang 1 („Beschreibung der Verarbeitungstätigkeiten“).
(3) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Die Regelungen dieses Vertrags gelten für alle Verarbeitungsvorgänge, die im Zusammenhang mit der Durchführung des Hauptvertrags erfolgen, sowie – soweit erforderlich – für darüber hinausgehende Aufbewahrungs- und Löschfristen.

§ 2 Art und Zweck der Verarbeitung, Kategorien von Daten und betroffenen Personen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zu folgenden Zwecken:
- Bereitstellung und Betrieb der vereinbarten IT-Infrastruktur- und Cloud-Services,
- Bereitstellung und Betrieb von Plattform- und Anwendungsdiensten, einschließlich „mIT Office“,
- optionale Bereitstellung von KI-bezogenen Infrastruktur- und Plattformdiensten (vgl. § 2a),
- Support-, Wartungs- und Administrationsleistungen,
- Sicherstellung der Verfügbarkeit, Integrität und Sicherheit der Systeme (z.B. Backups, Monitoring, Logging).

(2) Die Art der verarbeiteten personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich im Einzelnen aus Anhang 1. Dieser ist Bestandteil dieser Vereinbarung und wird vom Auftraggeber ausgefüllt und aktuell gehalten.
(3) Eine Verarbeitung personenbezogener Daten zu eigenen Zwecken des Auftragnehmers findet nicht statt. Ausgenommen hiervon sind ausschließlich gesetzlich zwingende Verarbeitungspflichten (z.B. gesetzliche Aufbewahrungspflichten, Auskunftspflichten gegenüber Behörden); der Auftragnehmer informiert den Auftraggeber hierüber, soweit rechtlich zulässig.

§ 2a Besondere Bestimmungen für KI-Services

(1) Soweit der Auftragnehmer dem Auftraggeber im Rahmen des Hauptvertrags Leistungen zur Bereitstellung von Infrastruktur- oder Plattformdiensten für den Betrieb von Anwendungen mit Komponenten künstlicher Intelligenz („KI-Services“) zur Verfügung stellt (z.B. KI-Gateway-Container, KI-Agent-Deployment, LLM-VM, Kubernetes-Cluster für LLMs), erfolgt die Verarbeitung personenbezogener Daten durch den Auftragnehmer ausschließlich im Rahmen dieser Vereinbarung und nach Weisung des Auftraggebers.
(2) Der Auftraggeber bleibt Verantwortlicher im Sinne der Art. 4 Nr. 7, 24 DS-GVO für alle Verarbeitungsvorgänge, die im Zusammenhang mit der Konzeption, Konfiguration und Nutzung der von ihm betriebenen KI-Anwendungen stehen. Dies umfasst insbesondere:
- die Auswahl und Konfiguration der eingesetzten KI-Modelle,
- die Festlegung der Zwecke, für die Eingabedaten und KI-Ergebnisse verwendet werden,
- die Einhaltung der gesetzlichen Anforderungen an den Einsatz von KI-Systemen (einschließlich des EU AI Act und einschlägiger Fachgesetze), soweit diese auf den Auftraggeber Anwendung finden.
(3) Gegenstand des Vertrags ist nicht die originäre Nutzung oder eigenständige Auswertung personenbezogener Daten durch den Auftragnehmer zu eigenen Zwecken, sondern ausschließlich die technische Bereitstellung, Konfiguration und der Betrieb der hierfür erforderlichen Infrastrukturkomponenten (z.B. Rechenleistung, Speicher, Netzwerke, Container-Plattform).
(4) Im Zuge der Leistungserbringung (Betrieb der Infrastruktur, Systemadministration, Support, Störungsbeseitigung) kann ein Zugriff des Auftragnehmers auf personenbezogene Daten nicht vollständig ausgeschlossen werden. Ein solcher Zugriff erfolgt ausschließlich zur Erfüllung der vertraglich geschuldeten Leistungen, auf dokumentierte Weisung des Auftraggebers und unter Beachtung der in dieser Vereinbarung und in Anhang 2 beschriebenen technischen und organisatorischen Maßnahmen.
(5) Der Auftraggeber stellt sicher, dass er sämtliche Informations-, Transparenz- und Dokumentationspflichten im Zusammenhang mit dem Einsatz der von ihm betriebenen KI-Anwendungen gegenüber betroffenen Personen erfüllt, insbesondere wenn KI-Systeme in eine Risikokategorie nach dem EU AI Act fallen.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DS-GVO). Der Hauptvertrag, diese Vereinbarung und die darin enthaltenen Leistungsbeschreibungen gelten als Weisung.
(2) Weisungen werden grundsätzlich schriftlich oder in Textform (z.B. per E-Mail, Ticketsystem) erteilt. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen; der Auftragnehmer dokumentiert mündliche Weisungen angemessen.
(3) Der Auftragnehmer prüft offensichtlich rechtswidrige Weisungen und informiert den Auftraggeber, wenn er eine Weisung für unzulässig hält. Der Auftragnehmer ist berechtigt, die Durchführung der Weisung bis zu einer Klarstellung oder Änderung durch den Auftraggeber auszusetzen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, die personenbezogenen Daten ausschließlich im Rahmen der Vereinbarung und der Weisungen des Auftraggebers zu verarbeiten und alle anwendbaren datenschutzrechtlichen Vorschriften zu beachten.

(2) Der Auftragnehmer stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen und zuvor in die datenschutzrechtlichen Anforderungen eingewiesen wurden.
(3) Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DS-GVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Zeitpunkt des Vertragsabschlusses bestehenden Maßnahmen sind in Anhang 2 beschrieben und Bestandteil dieser Vereinbarung.
(4) Der Auftragnehmer unterstützt den Auftraggeber, soweit möglich, mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten zur Beantwortung von Anträgen betroffener Personen und der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation von Aufsichtsbehörden).
(5) Der Auftragnehmer führt kein Verzeichnis der Verarbeitungstätigkeiten für den Auftraggeber; die Verantwortung hierfür liegt beim Auftraggeber. Soweit erforderlich, stellt der Auftragnehmer dem Auftraggeber die zur Führung des Verzeichnisses notwendigen Informationen zur Verfügung.

§ 5 Technisch-organisatorische Maßnahmen

(1) Die vom Auftragnehmer ergriffenen technisch-organisatorischen Maßnahmen zur Sicherstellung eines dem Risiko angemessenen Schutzniveaus, insbesondere Maßnahmen zur Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- sowie zur Trennungskontrolle, sind in Anhang 2 beschrieben.
(2) Der Auftragnehmer ist berechtigt, die vereinbarten Maßnahmen anzupassen und weiterzuentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die sich auf das Risiko für die Rechte und Freiheiten betroffener Personen auswirken, werden dem Auftraggeber in geeigneter Form mitgeteilt.

§ 6 Unterauftragsverhältnisse

(1) Der Einsatz von Unterauftragsverarbeitern („Subunternehmern“) ist nur mit Zustimmung des Auftraggebers und unter Abschluss einer Vereinbarung im Sinne von Art. 28 DS-GVO zulässig, die dem Subunternehmer dieselben Datenschutzpflichten auferlegt, wie sie in dieser Vereinbarung festgelegt sind.
(2) Die zum Zeitpunkt des Vertragsabschlusses eingesetzten Subunternehmer sind in Anhang 3 aufgelistet. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Subunternehmern und räumt dem Auftraggeber ein Widerspruchsrecht innerhalb einer angemessenen Frist ein.
(3) Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der datenschutzrechtlichen Pflichten durch die Subunternehmer, wie für eigenes Handeln.

§ 7 Unterstützung bei Betroffenenrechten

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Art. 12–22 DS-GVO), insbesondere bei Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch.

(2) Richtet sich ein Antrag betroffener Personen unmittelbar an den Auftragnehmer, leitet dieser den Antrag unverzüglich an den Auftraggeber weiter und nimmt eine Bearbeitung nur nach Weisung des Auftraggebers vor.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der in dieser Vereinbarung festgelegten datenschutzrechtlichen Anforderungen beim Auftragnehmer zu überprüfen, einschließlich durch Audits, Inspektionen oder Einsicht in einschlägige Zertifizierungen und Nachweisdokumente.
(2) Der Auftragnehmer ermöglicht dem Auftraggeber oder von diesem beauftragten Prüfern (die einer Vertraulichkeitsverpflichtung unterliegen) die Durchführung solcher Kontrollen in angemessenem Umfang sowie zu üblichen Geschäftszeiten unter Berücksichtigung der betrieblichen Abläufe.
(3) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten nachzuweisen.

Der Auftraggeber kann seine Kontrollrechte nach Abs. 1 und Abs. 2 anstelle einer Vor-Ort-Prüfung durch Vorlage und Einsichtnahme in aktuelle Zertifizierungs- und Testatberichte des Auftragnehmers ausüben, sofern diese den Gegenstand der Auftragsverarbeitung inhaltlich abdecken. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anfrage aktuelle Nachweise über bestehende Zertifizierungen, insbesondere das ISO 27001-Zertifikat sowie ggf. den BSI C5-Testatbericht, unverzüglich zur Verfügung zu stellen. Ein darüber hinausgehendes Recht auf physische Kontrolle bleibt unberührt, ist jedoch in diesem Fall nur dann geltend zu machen, wenn konkrete, dokumentierte Anhaltspunkte vorliegen, dass die Zertifizierungsnachweise den tatsächlichen Stand der Schutzmaßnahmen nicht zutreffend abbilden.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber unverzüglich jede ihm bekannt werdende Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung (Art. 33 DS-GVO). Die Meldung enthält mindestens die gesetzlich geforderten Informationen, soweit diese dem Auftragnehmer zum Zeitpunkt der Meldung vorliegen.
(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und gegebenenfalls betroffenen Personen.

§ 10 Löschung und Rückgabe von Daten nach Beendigung des Auftrags

(1) Nach Beendigung der vertraglichen Leistungen oder auf jederzeitige Weisung des Auftraggebers hin hat der Auftragnehmer sämtliche personenbezogenen Daten nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen, sofern der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
(2) Soweit der Auftraggeber keine Weisung erteilt, löscht der Auftragnehmer personenbezogene Daten nach Ablauf der im Hauptvertrag bzw. in den Leistungsbeschreibungen vereinbarten Vorhalte- und

Löschfristen.
(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, bewahrt der Auftragnehmer entsprechend den gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus auf. Sie werden dem Auftraggeber auf Wunsch überlassen.
(4) Soweit der Auftraggeber von seinem Recht auf Datenportabilität und Anbieterwechsel nach den Regelungen des Hauptvertrags und der darauf bezogenen Allgemeinen Geschäftsbedingungen der mitteldeutsche-IT GmbH (insbesondere AGB Cloud, Ziffer XII und XII.A) Gebrauch macht, löscht der Auftragnehmer die personenbezogenen Daten nach erfolgreichem Abschluss des vereinbarten Datenexports. Bis zum Abschluss des Datenexports verarbeitet der Auftragnehmer die personenbezogenen Daten ausschließlich zur Bereitstellung der hierfür erforderlichen technischen Leistungen und nach Weisung des Auftraggebers.

§ 11 Schlussbestimmungen

(1) Im Falle von Widersprüchen zwischen dieser Vereinbarung und den Regelungen des Hauptvertrags gehen die Bestimmungen dieser Vereinbarung denjenigen des Hauptvertrags vor, soweit es um den Datenschutz im Sinne der DS-GVO geht.
(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Dies gilt auch für die Änderung dieses Formerfordernisses.
(3) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden in diesem Fall die unwirksame Bestimmung durch eine wirksame Regelung ersetzen, die ihrem wirtschaftlichen Zweck möglichst nahekommt.

Datum des Inkrafttretens dieser Vereinbarung ist: 16.09.2026

Für den Auftragnehmer:

Martin Flechsig

Martin Flechsig
Geschäftsführer
mitteldeutsche-IT GmbH

Für den Auftraggeber:

Laura Hermes
Marketing
Test für Laura

Datenschutzbeauftragter auf Seiten der mitteldeutschen IT GmbH

mitteldeutsche IT GmbH
Thomas Ebell
Datenschutz und Compliance

datenschutz@mitteldeutsche-it.de
+4917624510498

Anhang 1 – Beschreibung der Verarbeitungstätigkeiten

Dieser Anhang ist Bestandteil der Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zwischen dem Auftraggeber und der mitteldeutsche-IT GmbH. Die Angaben unter Abschnitt 1 stellen den von der mitteldeutsche-IT GmbH vorausgefüllten Standard dar und sind vom Auftraggeber zu prüfen und bei Bedarf zu ergänzen. Die Angaben unter Abschnitt 2 (mIT Office) und Abschnitt 3 (KI-Services) gelten nur, sofern diese Leistungen im Hauptvertrag vereinbart wurden.

Abschnitt 1 – Allgemeine Cloud- und Infrastruktur-Services (IaaS / PaaS / SaaS)

1. Gegenstand der Verarbeitung

Gegenstand ist die Bereitstellung und der Betrieb von Cloud-Infrastruktur- und Plattformleistungen (Infrastructure as a Service / IaaS, Platform as a Service / PaaS, Software as a Service / SaaS) durch die mitteldeutsche-IT GmbH für den Auftraggeber. Die mitteldeutsche-IT GmbH stellt dem Auftraggeber virtuelle Server, Speicherkapazitäten, Netzwerkkomponenten und zugehörige Systemdienste in ihren Rechenzentren in Deutschland zur Verfügung. Im Rahmen des laufenden Betriebs (Systemadministration, Support, Backup, Monitoring, Logging, Störungsbeseitigung) kann ein technisch bedingter Zugriff auf personenbezogene Daten des Auftraggebers nicht vollständig ausgeschlossen werden.

Die mitteldeutsche-IT GmbH erstellt über die Funktion Data Loss Prevention (DLP) in der Regel täglich eine blockbasierte Sicherungskopie der Daten auf den virtuellen Systemen des Auftraggebers. Diese Sicherungskopien werden auf Speichermedien der mitteldeutsche-IT GmbH für die vertraglich vereinbarte Vorhaltezeit (Standard: 7 Tage; abweichende Vorhaltezeiten nach Leistungsschein) gespeichert. Beim Löschen des virtuellen Systems oder der virtuellen Instanz werden auch die zugehörigen Sicherungskopien gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

2. Zweck der Verarbeitung

- Bereitstellung und Betrieb der vom Auftraggeber gebuchten IT-Infrastruktur (virtuelle Server, Speicher, Netzwerke, Betriebssysteme)
- Systemadministration, Wartung und technischer Support
- Datensicherung (Backup / DLP) und Wiederherstellung
- Monitoring, Logging und Sicherstellung der Systemverfügbarkeit, -integrität und -sicherheit
- Störungsanalyse und -beseitigung

3. Kategorien personenbezogener Daten

Die im Rahmen der Cloud-Infrastruktur verarbeiteten personenbezogenen Daten ergeben sich aus dem jeweiligen Einsatz durch den Auftraggeber. Typischerweise handelt es sich um folgende Datenkategorien:

- Adress- und Kontaktdaten
- Dienstliche Mitarbeiterdaten (z. B. Name, Funktion, Erreichbarkeit)
- Authentifizierungs- und Zugangsdaten (z. B. Benutzernamen, Passwort-Hashes, Rollen)
- Stamm- und Konfigurationsdaten
- Transaktions- und Nutzungsdaten (z. B. Log-Dateien, Zugriffsprotokolle)
- Kommunikationsdaten (z. B. E-Mail-Metadaten, soweit auf Infrastrukturebene verarbeitet)
- Abrechnungs- und Leistungsdaten

Besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO werden im Rahmen der Standard-Infrastrukturleistungen grundsätzlich nicht verarbeitet. Soweit der Auftraggeber solche Daten auf der Infrastruktur verarbeitet, ist dies gesondert zu dokumentieren und dem Auftragnehmer mitzuteilen.

4. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers
- Kunden und Interessenten des Auftraggebers
- Lieferanten und Dienstleister des Auftraggebers
- Nutzer der durch den Auftraggeber betriebenen Anwendungen
- Sonstige natürliche Personen, deren Daten der Auftraggeber auf der Infrastruktur verarbeitet

5. Speicherorte und Vorhaltezeiten

Die Verarbeitung erfolgt ausschließlich in Rechenzentren der mitteldeutsche-IT GmbH in Deutschland (Standort: Leipzig). Eine Verarbeitung außerhalb der Europäischen Union findet nicht statt.

Datenart	Vorhaltezeit	Grundlage
Produktivdaten (VM-Speicher)	Laufzeit des Vertrags + Löschfrist nach Vertragsende	Hauptvertrag / AGB Cloud
DLP-Sicherungskopien	Standard: 7 Tage (anpassbar per Leistungsschein)	BVB mIT Cloud §5
System- und Zugriffslogs	Standard: 30 Tage (anpassbar per Leistungsschein)	BVB mIT Cloud, TOM-Dokumentation
Auftragsnachweise / Protokolle	Dauer gesetzlicher Aufbewahrungsfristen	§10 Abs. 3 AVV

Abschnitt 2 – Verarbeitung im Rahmen von „mIT Office" (SaaS)

Gilt nur, sofern der Auftraggeber den Cloud-Service „mIT Office" gebucht hat.

1. Gegenstand der Verarbeitung

Bereitstellung und Betrieb des SaaS-Dienstes „mIT Office" (insbesondere E-Mail, Kalender, Kontakte, gemeinsamer Dateispeicher, Kollaborationsfunktionen) für den Auftraggeber und seine Nutzer durch die mitteldeutsche-IT GmbH.

2. Zweck der Verarbeitung

- Betrieb der Kommunikations- und Kollaborationsfunktionen von mIT Office
- Verwaltung von Benutzerkonten und Zugriffsrechten
- Datensicherung, Systemmonitoring und Support
- Sicherstellung der Verfügbarkeit und Integrität der Dienste

3. Kategorien personenbezogener Daten

- E-Mail-Inhalte und -Anhänge
- Kalenderdaten (Termine, Einladungen, Teilnehmerinformationen)
- Kontaktdaten (Adressbücher, Verteilerlisten)
- Datei-Inhalte und zugehörige Metadaten in gemeinsam genutzten Speicherbereichen
- Benutzerkonten- und Authentifizierungsdaten (Benutzername, dienstliche E-Mail-Adresse, Rollen und Gruppen)
- Protokoll- und Nutzungsdaten (Anmeldeprotokolle, Zugriffsprotokolle, technische Ereignisprotokolle)

4. Kategorien betroffener Personen

- Beschäftigte und berechtigte Nutzer des Auftraggebers
- Externe Kommunikationspartner, mit denen der Auftraggeber über mIT Office kommuniziert

5. Speicherorte und Vorhaltezeiten

Die Verarbeitung erfolgt ausschließlich in Rechenzentren der mitteldeutsche-IT GmbH in Deutschland. Konkrete Vorhaltezeiten für Backups und Protokolldaten ergeben sich aus dem Leistungsschein mIT Office sowie den BVB mIT Cloud.

Abschnitt 3 – Verarbeitung im Rahmen von KI-Services

Gilt nur, sofern der Auftraggeber KI-bezogene Infrastruktur- oder Plattformdienste gemäß §2a AVV gebucht hat (z. B. KI-Gateway-Container, KI-Agent-Deployment, LLM-VM, Kubernetes-Cluster für LLMs).

1. Gegenstand der Verarbeitung

Bereitstellung und Betrieb technischer Infrastrukturkomponenten (Rechenleistung, Speicher, Netzwerke, Container-Plattform) zum Betrieb von KI-Anwendungen des Auftraggebers. Die Konfiguration, der fachliche Einsatz und die inhaltliche Nutzung der KI-Anwendungen sowie die Auswahl der KI-Modelle liegen in alleiniger Verantwortung des Auftraggebers.

2. Zweck der Verarbeitung (durch die mitteldeutsche-IT GmbH als Auftragsverarbeiter)

- Betrieb der vereinbarten KI-Infrastrukturkomponenten
- Systemadministration, Monitoring, Support und Störungsbeseitigung
- Datensicherung der Infrastrukturkomponenten

Hinweis: Eine eigenständige Nutzung oder Auswertung der in KI-Anwendungen verarbeiteten personenbezogenen Daten durch die mitteldeutsche-IT GmbH findet nicht statt.

3. Kategorien personenbezogener Daten

Die im Rahmen der KI-Infrastruktur verarbeiteten personenbezogenen Daten bestimmen sich nach dem KI-Anwendungsszenario des Auftraggebers. Vom Auftraggeber zu konkretisieren:

[Vom Auftraggeber auszufüllen: Welche personenbezogenen Daten werden als Eingabedaten (Prompts, Dokumente, Anfragen) in die KI-Anwendung eingebracht? Beispiel: Mitarbeiterkommunikation, Kundentickets, Vertragsunterlagen, Support-Anfragen.]

4. Kategorien betroffener Personen

[Vom Auftraggeber auszufüllen: Beispiel: Mitarbeiter, Kunden, Lieferanten.]

5. Speicherorte und Vorhaltezeiten

Die Verarbeitung erfolgt ausschließlich in Rechenzentren der mitteldeutsche-IT GmbH in Deutschland. Eingabedaten (Prompts) und Ausgabedaten werden nicht dauerhaft durch die mitteldeutsche-IT GmbH gespeichert, sofern dies nicht für den Betrieb der Infrastruktur technisch erforderlich ist. Konkrete Logging- und Vorhaltezeiten ergeben sich aus dem Leistungsschein und den BVB KI.

Anhang 2 – Technisch-organisatorische Maßnahmen (TOM)

Die zum Zeitpunkt des Vertragsabschlusses umgesetzten technischen und organisatorischen Maßnahmen sind im Dokument „Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO – mitteldeutsche-IT GmbH“ beschrieben. Dieses Dokument ist Bestandteil dieser Vereinbarung.

Anhang 3 – Subunternehmer / Unterauftragsverarbeiter

Gemäß § 6 dieser Vereinbarung zur Auftragsverarbeitung

Die **mitteldeutsche IT GmbH** (Auftragsverarbeiter) setzt bei der Erbringung der vertragsgegenständlichen Leistungen – insbesondere beim Betrieb von Cloud-Infrastrukturen, Managed Services und KI-Services – die nachfolgend aufgeführten Unterauftragsverarbeiter ein.

Alle Unterauftragsverarbeiter sind vertraglich verpflichtet, die Anforderungen der DS-GVO einzuhalten, insbesondere die technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO umzusetzen. Die Rechenzentren erfüllen branchenübliche Sicherheits- und Qualitätsstandards (u. a. ISO/IEC 27001 für Informationssicherheits-Management, DIN EN 50600 für Datacenter-Infrastrukturen) und sind teilweise als **kritische Infrastruktur** (KRITIS) gemäß BSI-Katalog eingestuft bzw. unterliegen der **NIS-2-Richtlinie**.

Der Auftragnehmer informiert den Auftraggeber gemäß § 6 dieser Vereinbarung über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern). Der Auftraggeber hat das Recht, aus wichtigem Grund innerhalb der vertraglich festgelegten Frist (i. d. R. 10 Werktage) Widerspruch zu erheben.

Rechenzentrum 1

Firmenname	envia TEL GmbH – Datacenter Leipzig II (Datacenter Deutschland)
Anschrift (Firmensitz)	envia TEL GmbH Friedrich-Ebert-Str. 26 04416 Markkleeberg
Funktion	Haupt-Data-Center / primärer Datacenter-Standort für Cloud- und Managed-Services der mitteldeutsche IT GmbH
Standort der Datenverarbeitung	Datacenter Leipzig II (DCL II) Leipziger Str. 116a 04425 Taucha bei Leipzig
Wichtige IT-Komponenten	Computing (Server/VM-Cluster), Storage-Systeme (SAN/NAS), Netzwerk-Management, System-Monitoring, Backup- und Recovery-Infrastruktur
Zertifizierungen	- **DIN EN 50600** (Datacenter Leipzig II, Verfügbarkeitsklasse VK3, Schutzklassen SK1–SK3, TÜV-zertifiziert) - **ISO/IEC 27001:2013** (Informationssicherheits-Management) - **ISO 9001:2015** (Qualitätsmanagement) - **ISO/IEC 22237** (internationale Rechenzentrumsnorm inkl. Energieeffizienz/Nachhaltigkeit) - **TÜViT Level 3** (TSI.STANDARD, hohe Verfügbarkeit und Sicherheit) - **KRITIS-Einstufung** gemäß BSI-Katalog (IT-Infrastruktur) - **NIS-2-Compliance** (EU-Richtlinie für Netz- und Informationssicherheit)
Datenschutzbeauftragter / Kontakt	envia TEL GmbH Abteilung Datenschutz Friedrich-Ebert-Str. 26 04416 Markkleeberg E-Mail: **DS@enviaTEL.de**
Notruf / 24/7-Störungsannahme	**0800 010 16 00** (Datacenter / Network Operations Center)
Allgemeiner Kontakt	E-Mail: **ticket@enviatel.de** Web: **https://www.enviatel.de**
Gegenstand der Unterbeauftragung	Bereitstellung und Betrieb der primären Datacenter-Infrastruktur (Colocation, Rack-Stellplätze, redundante Stromversorgung [2N-Konfiguration], Präzisions-Klimatisierung, physische Zutrittskontrolle [24/7-Überwachung, Videoüberwachung, Besuchermanagement], Brandschutz, Glasfaser-/IP-Netzwerkanbindungen) sowie Network Operations Center (NOC) für die von der mitteldeutsche IT GmbH betriebenen Cloud-, Managed- und KI-Service-Plattformen.
Rolle im Gesamtkonzept	**Haupt-Data-Center** / primärer Verarbeitungs- und Speicherort der Kundendaten. Weitere Rechenzentren (siehe unten) werden ausschließlich als **sekundäre bzw. Backup-Standorte** zur Erhöhung von Verfügbarkeit, Redundanz und Resilienz genutzt.
Rechtsgrundlage	Unterauftragsverarbeitungsvertrag gemäß Art. 28 Abs. 2–4 DS-GVO

Rechenzentrum 2

Firmenname	Avacon Connect GmbH / envia TEL GmbH (Datacenter Deutschland – gemeinsames Angebot)
Anschrift (Firmensitz Avacon Connect)	Peiner Str. 47 30880 Laatzen
Funktion	Datacenter-Betrieb / Colocation / **Backup-Standort**
Standort der Datenverarbeitung	Leipziger Str. 116a, 04425 Taucha (Rechenzentrum Leipzig, weiteres Gebäude/Segment des Datacenter-Campus)
Wichtige IT-Komponenten	Computing (Server, VMs), Storage (SAN/NAS), Netzwerk-Management, System-Monitoring, Backup-Infrastruktur
Zertifizierungen	- **DIN ISO/IEC 27001:2022** (Informationssicherheits-Management) - **DIN ISO 9001:2015** (Qualitätsmanagement) - **DIN EN 50600** (Datacenter-Infrastruktur, KRITIS-konform) - **KRITIS-Einstufung** gemäß BSI-Katalog (IT-Infrastruktur)
Datenschutzbeauftragter	envia TEL GmbH Abteilung Datenschutz Friedrich-Ebert-Str. 26 04416 Markkleeberg E-Mail: **DS@enviaTEL.de**
Notruf / 24/7-Störungsannahme	**0800 010 16 00** (Datacenter Network Operations)
Allgemeiner Kontakt	E-Mail: **ticket@enviatel.de** Web: **https://www.enviatel.de**
Gegenstand der Unterbeauftragung	Bereitstellung und Betrieb von redundanter Datacenter-Infrastruktur (Colocation, Rack-Stellplätze, redundante Stromversorgung und Klimatisierung, physische Zutrittskontrolle, Brandschutz, IP-Netzwerk/Dark Fiber) für **Backup- und Failover-Systeme** der vom Auftragsverarbeiter betriebenen Cloud- und Managed-Service-Plattformen.
Rolle im Gesamtkonzept	**Sekundärer / Backup-Standort** zur Erhöhung von Verfügbarkeit und Resilienz (georedundante Datensicherung, Disaster Recovery).
Rechtsgrundlage	Unterauftragsverarbeitungsvertrag gemäß Art. 28 Abs. 2–4 DS-GVO

Rechenzentrum 3

Firmenname	Digital Realty Germany GmbH (Rechenzentrum „Interxion Frankfurt FRA4 / FRAU4")
Anschrift	Hanauer Landstraße 298 60314 Frankfurt am Main
Funktion	Datacenter-Betrieb / Carrier-neutrale Colocation / **Backup-Standort**
Standort der Datenverarbeitung	Hanauer Landstraße 298 60314 Frankfurt am Main
Wichtige IT-Komponenten	Computing (Server, VMs), Storage (SAN/NAS), Netzwerk-Management, System-Monitoring, Backup-Infrastruktur
Zertifizierungen (Rechenzentrumsverbund)	- **ISO/IEC 27001:2013/2022** (Informationssicherheits-Management) - **ISO 22301:2019** (Business Continuity Management) - **ISO 14001:2015** (Umweltmanagement) - **ISO 50001:2018** (Energiemanagement) - **PCI DSS** (Payment Card Industry Data Security Standard) - **Compliance:** GDPR/DS-GVO, NIS-2-Richtlinie *Hinweis: Zertifizierungen gelten teils auf EU-/Regions- bzw. Unternehmensebene für Digital Realty-Standorte; Detailnachweise auf Anfrage beim Betreiber.*
Datenschutzbeauftragter (DPO)	DP Dock DPO Services GmbH Attn: Digital Realty Grüffkamp 10 24159 Kiel E-Mail: **digitalrealty@dp-officer.com**
Notruf / 24/7-Störungshotline	**+49 69 401 47 0** (Datacenter Operations Hotline)
Allgemeiner Kontakt	Web: **https://www.digitalrealty.de**
Gegenstand der Unterbeauftragung	Standort-Spezifikation: FRA4 / Hanauer Landstraße 298 Bereitstellung und Betrieb hochverfügbarer Datacenter-Infrastruktur (Colocation, Rack-Stellplätze, redundante Stromversorgung [2N], Präzisions-Klimatisierung, physische Sicherheit [Zutrittskontrollen, Videoüberwachung, Brandfrüherkennung], Carrier-neutrale Konnektivität) für **Backup- und Disaster-Recovery-Systeme** der vom Auftragsverarbeiter betriebenen Cloud-Plattformen.
Rolle im Gesamtkonzept	**Sekundärer / Backup-Standort** zur Erhöhung von Verfügbarkeit und Resilienz (georedundante Datensicherung, Disaster Recovery, Lastverteilung bei Notfällen).
Rechtsgrundlage	Unterauftragsverarbeitungsvertrag gemäß Art. 28 Abs. 2–4 DS-GVO

Hinweise

1. **Änderungsmitteilung:** Der Auftragnehmer informiert den Auftraggeber gemäß § 6 dieser Vereinbarung den Verantwortlichen über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern in Schrift- oder Textform. Die Information erfolgt in einer angemessenen Frist, die – im Sinne dieser Vereinbarung – 30 Kalendertage nicht unterschreiten soll.
   Der Verantwortliche kann aus wichtigem Grund gegen die beabsichtigte Änderung Einwände erheben. Erfolgt innerhalb der genannten Frist kein Einwand, gilt die Beauftragung des jeweiligen Unterauftragsverarbeiters als genehmigt.

2. **Weitere Subunternehmer für Nebenleistungen:** Nebenleistungen ohne direkten Zugriff auf personenbezogene Daten des Auftraggebers (z. B. allgemeine Wartung, Reinigung, Sicherheitsdienste, Logistik, Telekommunikationsdienstleister für IP-Transit) gelten gemäß § 6 Abs. 2 dieser Vereinbarung nicht als Unterauftragsverarbeiter im Sinne der DS-GVO und werden hier nicht aufgeführt.

3. **Audit-Rechte:** Der Auftraggeber kann gemäß § 3 dieser Vereinbarung Kontrollen und Audits bei Unterauftragsverarbeitern durchführen oder durch beauftragte Dritte durchführen lassen, soweit dies zur Erfüllung seiner Kontrollpflichten nach Art. 28 Abs. 3 lit. h DS-GVO erforderlich ist.

4. **Datenverarbeitung ausschließlich in der EU:** Sämtliche Unterauftragsverarbeiter verarbeiten personenbezogene Daten ausschließlich innerhalb der Bundesrepublik Deutschland bzw. der Europäischen Union. Eine Verarbeitung außerhalb der EU/EWR erfolgt nicht.

Stand dieser Anlage: 14.03.2026