Auftragsverarbeitungsvertrag gemäß Artikel 28 DSGVO

zwischen (der)

_____
_____
_____
_____

Name und Anschrift des Vertragspartners
- Verantwortlicher im Sinne der DSGVO, im Folgenden Auftraggeber -

und der

P-CATION Consulting and Solutions GmbH
Kirchstraße 44
59823 Arnsberg
Deutschland
- Auftragsverarbeiter im Sinne der DSGVO, im Folgenden Auftragnehmer -

Einleitung

Dieser Auftragsverarbeitungsvertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den mit dem Hauptvertrag in Verbindung stehenden Verarbeitungstätigkeiten ergeben. Der AV-Vertrag gilt für alle Tätigkeiten, die im Rahmen des Hauptvertrags erfolgen und bei denen Beschäftigte des Auftragnehmers oder von ihm beauftragte Dritte personenbezogene Daten im Auftrag des Auftraggebers verarbeiten.

§ 1 Gegenstand und Dauer der Verarbeitung

1. Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Software-as-a-Service-Plattform "LIVOI".
2. Zweck der Verarbeitung ist die technische Bereitstellung, der Betrieb, die Wartung und der Support der Plattform einschließlich KI-gestützter Kommunikations- und Automatisierungsprozesse sowie der vom Auftraggeber konfigurierten Nutzung externer Kommunikations- und Wissensquellen.
3. Art der Verarbeitung umfasst insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten personenbezogener Daten, soweit dies zur Erfüllung des Hauptvertrages, zum Betrieb der Plattform, zur Bearbeitung von Supportanfragen sowie zur Durchführung der vom Auftraggeber konfigurierten Kommunikations- und Automatisierungsprozesse erforderlich ist.
4. Der Auftragnehmer stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
5. Die Verarbeitung erfolgt ausschließlich nach dokumentierter Weisung des Auftraggebers.
6. Die Dauer dieses Vertrages entspricht der Laufzeit des zugrunde liegenden Hauptvertrages.

§ 2 Art und Zweck der Verarbeitung, Art der Daten und Kategorien betroffener Personen

1. Art und Zweck der Verarbeitung bestimmen sich nach § 1 Abs. 2 und 3 sowie ergänzend nach Anlage 1 zu diesem Vertrag.
2. Die Art der verarbeiteten personenbezogenen Daten sowie die Kategorien der betroffenen Personen ergeben sich aus Anlage 1 zu diesem Vertrag.
3. Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist nicht Gegenstand dieses Vertrages.

§ 3 KI-spezifische Regelungen

1. Der Auftragnehmer bietet die Möglichkeit, im Rahmen von LIVOI KI-Modelle (Large Language Models) einzusetzen, um die vom Auftraggeber vorgesehenen Kommunikations- und Automatisierungsfunktionen technisch zu realisieren.
2. Eine Nutzung personenbezogener Daten des Auftraggebers oder der betroffenen Personen zum Training, zur Weiterentwicklung oder zur Verbesserung von KI-Modellen findet nicht statt.
3. **3.** Die Verarbeitung durch KI-Modelle erfolgt ausschließlich zweckgebunden zur Generierung konkreter Antworten oder Verarbeitungsschritte im jeweiligen Nutzungskontext. Die im Rahmen dieses Vertrages vorgesehenen Verarbeitungs- und Speichervorgänge (insbesondere Speicherung in LIVOI gemäß § 1 und Anlage 2) bleiben hiervon unberührt.
4. Der Einsatz externer KI-Dienste sowie die Freischaltung bestimmter KI-Modelle oder Modellklassen erfolgen nur, soweit dies im Hauptvertrag, in Anlage 3, durch die vom Auftraggeber vorgenommene Konfiguration oder durch eine dokumentierte Weisung des Auftraggebers vorgesehen ist. Der Auftragnehmer beschränkt die Auswahl auf Dienste, für die geeignete vertragliche und technische Garantien bestehen, dass übermittelte Daten nicht zu eigenen Zwecken, insbesondere nicht zum Training oder zur Verbesserung von KI-Modellen, verwendet werden.
5. Zu den KI-bezogenen technischen und organisatorischen Maßnahmen zählen insbesondere die rollenbasierte Freischaltung von KI-Funktionen, die Beschränkung der Datenübermittlung an freigegebene Dienste und Modelle, die Protokollierung von Änderungen an KI-Konfigurationen, die verschlüsselte Übermittlung an externe KI-Dienste sowie die mandantenbezogene Zugriffstrennung. Ergänzend gelten die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen, insbesondere Ziff. 2.5 und Ziff. 6.

§ 4 Weisungen des Auftraggebers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch gesetzliche Vorschriften zu einer anderen Verarbeitung verpflichtet ist.
2. Die bei Vertragsschluss maßgeblichen Weisungen des Auftraggebers sind in diesem Vertrag und seinen Anlagen dokumentiert.
3. Weitere Weisungen sowie Änderungen oder Ergänzungen bestehender Weisungen sind mindestens in Textform (z. B. per E-Mail, Ticketsystem oder sonstige dokumentierbare elektronische Kommunikation) an die von den Parteien benannten Ansprechpartner zu übermitteln. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
4. Der Auftragnehmer dokumentiert den Eingang, den Inhalt und die Umsetzung von Weisungen in angemessener Weise.
5. Weisungen innerhalb des vertraglich vereinbarten Leistungs- und Verarbeitungsumfangs sind verbindlich und vom Auftragnehmer unverzüglich beziehungsweise innerhalb angemessener Frist umzusetzen.
6. Weisungen, die über den vertraglich vereinbarten Leistungs- oder Verarbeitungsumfang hinausgehen oder zusätzliche technische, organisatorische oder personelle Maßnahmen erfordern, gelten als Änderungsverlangen. Der Auftragnehmer wird den Auftraggeber unverzüglich auf den hierdurch entstehenden Mehraufwand und eine etwaige zusätzliche Vergütung hinweisen; die datenschutzrechtliche Weisungsgebundenheit innerhalb des vereinbarten Leistungsumfangs bleibt unberührt.
7. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich und ist berechtigt, die Ausführung der Weisung bis zur Bestätigung oder Anpassung auszusetzen.

§ 5 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Diese ergeben sich aus Anlage 2 zu diesem Vertrag.
2. Der Auftragnehmer ist berechtigt, die technischen und organisatorischen Maßnahmen während der Laufzeit dieses Vertrages anzupassen oder weiterzuentwickeln, sofern hierdurch das vereinbarte Schutzniveau nicht unterschritten wird.
3. Der Auftraggeber erhält auf Anforderung die erforderlichen Informationen zum Nachweis der Einhaltung der Maßnahmen.

§ 6 Einsatz weiterer Auftragsverarbeiter

1. Der Auftragnehmer ist berechtigt, weitere Auftragsverarbeiter einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Auftragsverarbeiter sind in Anlage 3 aufgeführt.
2. Der Auftragnehmer informiert den Auftraggeber in Textform mindestens 14 Kalendertage vor beabsichtigten Änderungen hinsichtlich der Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter.
3. Der Auftraggeber ist berechtigt, innerhalb von 14 Kalendertagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund Widerspruch einzulegen.
4. In der Mitteilung nach Abs. 2 weist der Auftragnehmer den Auftraggeber besonders darauf hin, dass ein ausbleibender Widerspruch innerhalb der Frist als Zustimmung gilt. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung als erteilt.
5. Im Falle eines berechtigten Widerspruchs werden die Parteien unverzüglich prüfen, ob die Leistungen ohne den betroffenen weiteren Auftragsverarbeiter oder unter Einsatz eines datenschutzrechtlich und wirtschaftlich zumutbaren alternativen weiteren Auftragsverarbeiters fortgeführt werden können. Ist dies objektiv nicht möglich oder dem Auftragnehmer nicht zumutbar, kann jede Partei den von der Änderung betroffenen Leistungsteil oder, wenn eine Trennung nicht möglich ist, den Hauptvertrag mit angemessener Frist aus wichtigem Grund kündigen.
6. Sofern Auftragsverarbeiter in Drittstaaten eingesetzt werden, erfolgt dies ausschließlich unter Einhaltung der Art. 44 ff. DSGVO, insbesondere auf Grundlage der EU-Standardvertragsklauseln (Modul 3) oder eines anwendbaren Angemessenheitsbeschlusses.
7. Der Auftragnehmer schließt mit jedem weiteren Auftragsverarbeiter vor Beginn der Verarbeitung einen Vertrag nach Art. 28 Abs. 4 DSGVO (Auftragsverarbeitungsvertrag / Data Processing Addendum) ab. Dieser Vertrag hat dem weiteren Auftragsverarbeiter mindestens solche Datenschutzpflichten aufzuerlegen, die den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen und ein dem vorliegenden Vertrag im Wesentlichen gleichwertiges Schutzniveau sicherstellen, insbesondere hinsichtlich Vertraulichkeit, technischer und organisatorischer Maßnahmen, Unterstützungspflichten, Meldepflichten bei Datenschutzverletzungen sowie Löschung oder Rückgabe nach Vertragsende.
8. Der Auftragnehmer stellt sicher, dass ihm gegenüber dem weiteren Auftragsverarbeiter die zur Erfüllung seiner Nachweis- und Kontrollpflichten erforderlichen Informations- und Prüfrechte zustehen. Soweit unmittelbare Vor-Ort-Überprüfungen des Auftraggebers beim weiteren Auftragsverarbeiter rechtlich oder tatsächlich nicht durchsetzbar sind, stellt der Auftragnehmer dem Auftraggeber auf Anforderung geeignete Nachweise (z. B. Zertifizierungen, Auditberichte, Testate oder Berichte unabhängiger Dritter) zur Verfügung und unterstützt angemessene alternative Prüfungsmaßnahmen. Unmittelbare Vor-Ort Inspektionen des Auftraggebers beim

weiteren Auftragsverarbeiter erfolgen nur, soweit dies vertraglich durchsetzbar ist und dem keine überwiegenden Geheimhaltungs-, Sicherheits- oder Rechtsgründe entgegenstehen. Die Regelungen in § 10 Abs. 2 bis 7 gelten entsprechend.

9. Der Auftragnehmer bleibt dem Auftraggeber gegenüber für die Erfüllung der Datenschutzpflichten des weiteren Auftragsverarbeiters verantwortlich.

§ 7 Unterstützungspflichten / Rechte betroffener Personen

1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen gemäß Kapitel III DSGVO (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch).
2. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach dokumentierter Weisung des Auftraggebers und nimmt keine eigenständige Beauskunftung, Berichtigung, Löschung oder Einschränkung der Verarbeitung vor.
3. Soweit sich eine betroffene Person unmittelbar an den Auftragnehmer wendet, leitet dieser das entsprechende Ersuchen unverzüglich an den Auftraggeber weiter.
4. Der Auftragnehmer unterstützt den Auftraggeber nach besten Kräften bei der Erfüllung seiner Pflichten gegenüber Datenschutzaufsichtsbehörden, insbesondere im Rahmen von:
    a. Anfragen, Untersuchungen oder Prüfungen durch Aufsichtsbehörden,
    b. Ordnungswidrigkeits- oder Strafverfahren,
    c. Haftungs- oder Beschwerdeverfahren betroffener Personen, soweit diese im Zusammenhang mit der Auftragsverarbeitung stehen.
5. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Einhaltung seiner gesetzlichen Pflichten, soweit diese die Verarbeitung nach diesem Vertrag betreffen. Dies umfasst insbesondere die Unterstützung bei der Umsetzung und Einhaltung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO. Der Auftragnehmer wirkt auf Anfrage an der Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DSGVO) des Auftraggebers mit, soweit die Verarbeitung nach diesem Vertrag betroffen ist, und stellt die hierzu erforderlichen Informationen zur Verfügung.
6. Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO oder zur vorherigen Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO verpflichtet ist, unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Der Auftragnehmer wirkt auf Anfrage an der Erstellung sowie Aktualisierung der Datenschutz-Folgenabschätzung und der hierfür erforderlichen Unterlagen mit und legt dem Auftraggeber alle hierfür erforderlichen Angaben und Dokumente auf Anfrage offen, soweit diese dem Auftragnehmer vorliegen oder von ihm zumutbar beschafft werden können. Betriebs- und Geschäftsgeheimnisse sind dabei zu wahren.

7. Der Auftragnehmer arbeitet auf Anfrage mit der zuständigen Datenschutzaufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen, soweit die Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages betroffen ist.

§ 8 Meldung von Datenschutzverletzungen

1. Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist.
2. Die Mitteilung enthält insbesondere:
    a. Art der Verletzung,
    b. Kategorien und Anzahl betroffener Personen,
    c. Kategorien und Anzahl betroffener Datensätze,
    d. wahrscheinliche Folgen,
    e. ergriffene oder vorgeschlagene Abhilfemaßnahmen.
3. Der Auftragnehmer dokumentiert Datenschutzverletzungen und stellt die Dokumentation dem Auftraggeber auf Anforderung zur Verfügung.

§ 9 Haftung und Freistellung

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Betroffenenrechte allein verantwortlich, soweit sich aus diesem Vertrag nichts anderes ergibt.
2. Der Auftraggeber stellt den Auftragnehmer auf erstes Anfordern von sämtlichen Ansprüchen Dritter frei, die gegen den Auftragnehmer wegen datenschutzrechtlicher Verstöße geltend gemacht werden, soweit diese ihre Ursache in einem Verhalten oder einer Pflichtverletzung des Auftraggebers haben.
3. Die Freistellung umfasst auch angemessene Rechtsverfolgungskosten.
4. Die Freistellungspflicht besteht nicht bei vorsätzlichem oder grob fahrlässigem Verhalten des Auftragnehmers.
5. Soweit gegen den Auftragnehmer Geldbußen oder sonstige Sanktionen verhängt werden, stellt der Auftraggeber den Auftragnehmer in dem Umfang frei, in dem der Auftraggeber für den sanktionierten Verstoß verantwortlich ist.
6. Im Übrigen gelten die Haftungsregelungen des Hauptvertrages entsprechend.

§ 10 Nachweise und Überprüfungen

1. Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrages zu überprüfen.
2. Der Auftragnehmer unterstützt den Auftraggeber bei solchen Überprüfungen in angemessenem Umfang und stellt die hierfür erforderlichen Informationen, Nachweise und Zugänge nach Maßgabe dieses Vertrages zur Verfügung.
3. Überprüfungen sind mindestens 14 Kalendertage im Voraus anzukündigen und während der üblichen Geschäftszeiten durchzuführen, soweit nicht ein dringender datenschutzrechtlicher Anlass eine kürzere Frist erfordert.
4. Der Auftraggeber ist grundsätzlich berechtigt, eine Vor-Ort-Überprüfung pro Kalenderjahr beim Auftragnehmer durchzuführen. Anlassbezogene Überprüfungen aus wichtigem Grund sowie Überprüfungen bei weiteren Auftragsverarbeitern nach Maßgabe von § 6 und unter Berücksichtigung der dort geregelten tatsächlichen und rechtlichen Grenzen bleiben hiervon unberührt.
5. Der Auftragnehmer ist berechtigt, den Nachweis der Einhaltung seiner Pflichten durch Vorlage geeigneter Zertifizierungen, Prüfberichte oder Audit-Testate zu erbringen.
6. Wettbewerber des Auftragnehmers dürfen nicht mit der Durchführung von Prüfungen beauftragt werden.
7. Betriebs- und Geschäftsgeheimnisse des Auftragnehmers und weiterer Auftragsverarbeiter sind zu wahren; Überprüfungen sind so durchzuführen, dass der Betriebsablauf und die Sicherheitssysteme nicht unangemessen beeinträchtigt werden.

§ 11 Vertragsdauer und Beendigung

1. Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages.
2. Die Beendigung des Hauptvertrages bewirkt automatisch die Beendigung dieses Vertrages.
3. Eine isolierte ordentliche Kündigung dieses Vertrages ist ausgeschlossen. Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn der Auftragnehmer schwerwiegend oder trotz angemessener Fristsetzung fortgesetzt gegen wesentliche Datenschutzpflichten aus diesem Vertrag verstößt.
4. Nach Beendigung dieses Auftragsverarbeitungsvertrags hat der Auftragnehmer nach Wahl des Auftraggebers sämtliche personenbezogenen Daten unverzüglich zu löschen oder - soweit technisch möglich und vertraglich vorgesehen - an den Auftraggeber in einem gängigen, maschinenlesbaren Format herauszugeben, sofern keine gesetzliche Verpflichtung zur weiteren Speicherung besteht. Soweit eine vollständige Rückgabe technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand verbunden ist, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich; in diesem Fall erfolgt die Löschung der Daten sowie die Herausgabe der beim Auftragnehmer in exportfähiger Form vorhandenen personenbezogenen

Daten. Gesetzliche Aufbewahrungspflichten bleiben unberührt. In diesem Fall werden die betroffenen personenbezogenen Daten für jede weitere Verarbeitung gesperrt und ausschließlich zur Erfüllung der gesetzlichen Aufbewahrungspflichten gespeichert. Nachweise über die ordnungsgemäße Verarbeitung personenbezogener Daten (z. B. Protokolle, Dokumentationen zu technischen und organisatorischen Maßnahmen oder Auditnachweise) dürfen über das Vertragsende hinaus aufbewahrt werden, soweit dies zur Erfüllung gesetzlicher oder regulatorischer Anforderungen erforderlich ist. Der Auftragnehmer bestätigt dem Auftraggeber auf Anforderung in Textform die Löschung beziehungsweise Rückgabe.

§ 12 Schlussbestimmungen

1. Im Falle von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen der Parteien gehen die Regelungen dieses Vertrages vor.
2. Maßgeblich ist ausschließlich die deutsche Fassung dieses Vertrages. Übersetzungen dienen lediglich Informationszwecken.
3. Änderungen und Ergänzungen dieses Vertrages einschließlich Nebenabreden sowie die Änderung oder Aufhebung dieser Klausel bedürfen mindestens der Textform, soweit nicht eine strengere gesetzliche Form vorgeschrieben ist.
4. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Zwingende datenschutzrechtliche Vorschriften bleiben unberührt.

Anlage 1 - Zweck, Art und Umfang der Datenverarbeitung sowie Art der Daten und Kategorien der betroffenen Personen

Zweck der Verarbeitung

- technische Bereitstellung, Betrieb, Wartung und Support der Plattform LIVOI,
- Durchführung der vom Auftraggeber konfigurierten Kommunikations- und Automatisierungsprozesse, einschließlich KI-gestützter Antwort- und Verarbeitungsschritte,
- Anbindung und Nutzung externer Kommunikations- und Wissensquellen sowie weiterer vom Auftraggeber freigegebener Integrationen.

Art und Umfang der Verarbeitung

- Erheben, Übernehmen, Erfassen, Strukturieren und Speichern personenbezogener Daten aus vom Auftraggeber bereitgestellten oder angebundenen Quellen,
- Auslesen, Abfragen, Verwenden, Übermitteln und Bereitstellen von Daten innerhalb der Plattform sowie an vom Auftraggeber aktivierte Kommunikationskanäle, Wissensquellen und Integrationen,
- Automatisierte Verarbeitungsschritte, einschließlich KI-Inferenz, zur Generierung von Antworten, Vorschlägen, Klassifizierungen oder sonstigen vom Auftraggeber ausgelösten Prozessschritten,
- Löschen, Sperren, Exportieren und sonstige Datenverwaltungsmaßnahmen auf Weisung des Auftraggebers.

Art der verarbeiteten Daten

- Stammdaten (z. B. Vor- und Nachname, Anzeigename)
- Kontaktdaten (z. B. E-Mail-Adresse, Telefonnummer)
- Kommunikationsdaten (z. B. Chat-Nachrichten, Konversationsverläufe)
- Nutzungs- und Protokolldaten (z. B. Login-Zeitpunkte, Systemereignisse)
- Inhaltsdaten aus vom Auftraggeber hochgeladenen oder angebundenen Dokumenten/Systemen
- Technische Metadaten (z. B. Zeitstempel, Berechtigungsstufen)

Kategorien betroffener Personen

- Kunden und Endkunden des Auftraggebers
- Mitarbeitende des Auftraggebers
- Ansprechpartner und Kommunikationspartner
- Sonstige personenbezogene Daten, die der Auftraggeber im Rahmen der vertragsgegenständlichen Verarbeitung verarbeitet

Anlage 2 - Technische und organisatorische Maßnahmen (TOMs) nach Artikel 32 DSGVO

1. Allgemeines Sicherheitskonzept

- Der Betrieb erfolgt auf der Infrastruktur der Hetzner Online GmbH in Deutschland. Die Rechenzentren sind nach ISO/IEC 27001 zertifiziert.
- Hetzner Technische und organisatorische Maßnahmen: https://www.hetzner.com/AV/TOM.pdf 2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Verschlüsselung - Datenübertragung (Data in Transit)

Sämtliche Kommunikation zwischen Client (Browser/Teams/WhatsApp), den LIVOI-Servern und Drittsystemen erfolgt ausschließlich über verschlüsselte Kanäle (TLS 1.2 oder höher).

2.2 Verschlüsselung - Datenspeicherung (Data at Rest)

Datenbanken:

Sensible Daten in den operativen Datenbanken (Hetzner) werden mittels AES-256 verschlüsselt. Sensible Identifikatoren, die im Klartext nicht mehr verwendet werden müssen (z. B. API Keys), werden zusätzlich gehasht (SHA-256).

Dateiablage / Object Storage:

Dokumente liegen in logisch getrennten Speicherbereichen (Buckets). Der Zugriff ist durch strikte Access Control Lists (ACLs) auf die Applikationsebene beschränkt. Der Zugriff erfolgt ausschließlich über zeitlich begrenzte, berechtigungsgebundene presigned URLs; ein öffentlicher oder dauerhafter URL-Zugriff ist ausgeschlossen. (Hinweis: Die Implementierung einer zusätzlichen Server-Side Encryption (SSE) zur vollständigen Verschlüsselung der ruhenden Dateien ist optional möglich). Unabhängig davon sind die Dateien bereits durch Zugriffsbeschränkungen und logische Mandantentrennung geschützt.

2.3 Mandantentrennung (Tenant Isolation)

Alle Daten innerhalb von LIVOI sind strikt mandantengetrennt. Die Trennung erfolgt auf Datenbankebene mittels Row-Level Security (RLS) Policies. Diese stellen sicher, dass Nutzer und Systeme ausschließlich auf Datensätze ihres eigenen Tenants zugreifen können. Ein tenantübergreifender Zugriff ist technisch ausgeschlossen und wird zusätzlich durch das Rollenkonzept sowie die Authentifizierungsschicht abgesichert.

2.4 Physische und logische Zugangskontrolle

Der physische Zugang zu den Datenverarbeitungsanlagen ist auf autorisierte Personen beschränkt und erfolgt in gesicherten Rechenzentren des Hosting-Dienstleisters. Zutrittskontrollen, Zugangsbeschränkungen, Besucherregelungen und Überwachungsmaßnahmen werden durch den Hosting-Dienstleister gemäß anerkannten Sicherheitsstandards umgesetzt. Der logische Zugang zu

den Systemen erfolgt ausschließlich über personalisierte Benutzerkonten. Zugriffsrechte werden rollenbasiert vergeben und regelmäßig überprüft. Authentifizierungs- und Autorisierungsmechanismen stellen sicher, dass nur berechtigte Nutzer Zugriff auf personenbezogene Daten erhalten. Geeignete Maßnahmen zur Absicherung von Benutzerkonten, insbesondere durch starke Authentifizierungsmechanismen und automatische Sperrmechanismen, sind implementiert.

2.5 KI-spezifische technische und organisatorische Maßnahmen

- KI-Funktionen und externe KI-Dienste werden nur für vom Auftraggeber freigegebene oder konfigurierte Anwendungsfälle aktiviert.
- Übermittlungen an externe KI-Dienste erfolgen ausschließlich zweckgebunden für einzelne Inferenzanfragen und über verschlüsselte Verbindungen.
- Änderungen an KI-Konfigurationen, Modellfreigaben und relevanten Schnittstellen werden protokolliert und sind auf berechtigte Personen beschränkt.
- Vor Einsatz externer KI-Dienste werden deren vertragliche Zusicherungen und Einstellungen darauf überprüft, dass keine Nutzung der übermittelten Daten zu eigenen Trainings- oder
- Verbesserungszwecken erfolgt.
- Für die Administration von KI-bezogenen Funktionen gilt ein rollenbasiertes Berechtigungskonzept; eine mandantenübergreifende Nutzung von Eingabedaten zu Trainingszwecken ist ausgeschlossen.

3. Datenlebenszyklus und Löschkonzept

Um dem Grundsatz der Datensparsamkeit und der Speicherbegrenzung gerecht zu werden, gelten folgende Regeln:

1. Zentrale Speicherung: Konversationen werden in der LIVOI-Datenbank (Hetzner, Deutschland) gespeichert, um den Kontext für Rückfragen zu erhalten.
2. Externe Kanäle (WhatsApp): Sofern der Kommunikationskanal WhatsApp genutzt wird, werden Nachrichten systembedingt auch über die Infrastruktur von Meta verarbeitet und auf den Endgeräten gespeichert. Die Übertragung erfolgt hierbei WhatsApp-konform (End-to-End-Verschlüsselung). Die Nutzung externer Kommunikationskanäle erfolgt ausschließlich auf Initiative und Konfiguration des Auftraggebers.
3. Recht auf Löschung: Das Recht auf Löschung (Art. 17 DSGVO) ist technisch vollumfänglich gewährleistet. Kunden können die Entfernung spezifischer Historien aus der LIVOI-Datenbank jederzeit veranlassen.
4. Integrität

   Zugriffe auf personenbezogene Daten unterliegen einem rollenbasierten Berechtigungskonzept. Änderungen an Systemkonfigurationen und sicherheitsrelevanten Komponenten werden protokolliert.

4.1 Weitergabe- und Eingabekontrolle

Die Übermittlung personenbezogener Daten erfolgt ausschließlich über gesicherte

Übertragungswege (z. B. TLS-verschlüsselte Verbindungen). Unbefugtes Lesen, Kopieren, Verändern oder Löschen während der Übertragung wird durch technische Schutzmaßnahmen verhindert. Eingaben, Änderungen und Löschungen personenbezogener Daten werden protokolliert und sind eindeutig einzelnen Benutzerkonten zuordenbar. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung erfolgt auf Grundlage eines rollenbasierten Berechtigungskonzepts.

5. Verfügbarkeit und Belastbarkeit

Der Betrieb erfolgt auf der Infrastruktur der Hetzner Online GmbH mit redundanter Auslegung. Regelmäßige Datensicherungen werden durchgeführt.

5.1 Wiederherstellbarkeit und Notfallmanagement

Es bestehen Verfahren zur regelmäßigen Datensicherung sowie zur Überwachung der Backup-Prozesse. Maßnahmen zur Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach technischen oder physischen Zwischenfällen sind definiert. Die Wiederherstellung der Daten wird regelmäßig getestet und dokumentiert. Für den Umgang mit Notfällen und Störungen bestehen abgestimmte Notfall- und Wiederanlaufkonzepte. Mindestens einmal pro Kalenderjahr führt der Auftragnehmer einen dokumentierten Disaster-Recovery-Test (Notfallwiederherstellung) der Datenbank durch (Wiederherstellung aus Backup in geeigneter Test-/Isolationsumgebung inklusive Integritätsprüfung). Eine Zusammenfassung beziehungsweise ein Protokoll des Tests wird dem Auftraggeber auf Anfrage zur Verfügung gestellt; Betriebs- und Geschäftsgeheimnisse sind zu wahren.

6. Datenschutzmanagement und Datenschutz durch Technikgestaltung

Der Auftragsverarbeiter hat organisatorische Maßnahmen zur Sicherstellung der Einhaltung der datenschutzrechtlichen Anforderungen implementiert. Hierzu gehören insbesondere:

- Verpflichtung der Mitarbeiter auf Vertraulichkeit und Datenschutz
- Regelmäßige Sensibilisierung und Schulung der Mitarbeiter
- Etablierte Prozesse zur Bearbeitung von Betroffenenanfragen
- Verfahren zur Erkennung, Bewertung und Meldung von Datenschutzverletzungen
- Berücksichtigung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO
- Unterstützung/Mitwirkung bei Datenschutz-Folgenabschätzungen, soweit erforderlich
- Benennung klarer Zuständigkeiten für Datenschutz und Informationssicherheit innerhalb der Organisation

Anlage 3 - Genehmigte Unterauftragsverhältnisse

Die in dieser Anlage genannten weiteren Auftragsverarbeiter werden nur insoweit eingesetzt, als dies für die vom Auftraggeber gebuchten, konfigurierten oder freigegebenen Funktionen erforderlich ist.

Soweit personenbezogene Daten an Unterauftragsverarbeiter in Drittstaaten übermittelt werden, erfolgt die Übermittlung auf Grundlage eines Angemessenheitsbeschlusses gemäß Art. 45 DSGVO, insbesondere des EU US Data Privacy Frameworks (DPF), sofern der jeweilige Anbieter für die relevanten Dienste zertifiziert ist.

Sofern kein Angemessenheitsbeschluss vorliegt oder dieser nicht anwendbar ist, erfolgt die Übermittlung auf Grundlage der Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO, insbesondere unter Verwendung des Moduls 3 (Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter).

Anbieter: Hetzner Online GmbH

Verarbeitungsvorgang: Hosting, Datenbankbetrieb, Storage

Ort der Verarbeitung: Deutschland (EU)

Art der Daten: Auftraggeber-Daten

Datenschutzrechtliche Grundlage: Auftragsverarbeitungsvertrag (AVV), ISO/IEC 27001 **Besondere Einschränkungen:** Verarbeitung ausschließlich innerhalb der Europäischen Union

Anbieter: Microsoft Ireland Operations Limited / Microsoft Corporation (Azure)

Verarbeitungsvorgang: Nachrichtentransport und optionale Integration von Microsoft Teams **Ort der Verarbeitung:** EU (Datenruhe); Drittland (USA) ausschließlich für Übertragungs- und Betriebsvorgänge im Rahmen globaler Bereitstellung

Art der Daten: Auftraggeber-Daten

Datenschutzrechtliche Grundlage: EU-US Data Privacy Framework (DPF) oder Standarddatenschutzklauseln (Modul 3), Data Processing Addendum (DPA)

Besondere Einschränkungen: Nutzung ausschließlich, soweit die entsprechende Integration vom Auftraggeber ausgewählt, aktiviert oder freigegeben wurde; keine Nutzung der Daten zu Trainings- oder Optimierungszwecken

Anbieter: OpenAI Ireland Ltd. / OpenAI, L.L.C.

Verarbeitungsvorgang: KI-Inferenz im Rahmen der Nutzung von Large Language Models (LLM API) **Ort der Verarbeitung:** EU (Datenruhe); gegebenenfalls Drittland (USA) ausschließlich für

KI-Inferenzanfragen **Art der Daten:** Kommunikations- und Inhaltsdaten
Datenschutzrechtliche Grundlage: EU-US Data Privacy Framework (DPF) oder Standarddatenschutzklauseln (Modul 3), Data Processing Addendum (DPA)

Besondere Einschränkungen: Einsatz ausschließlich, soweit die betreffende KI-Funktion oder das betreffende Modell vom Auftraggeber ausgewählt, aktiviert oder freigegeben wurde; keine Speicherung, Weiterverwendung oder Nutzung der Daten zu Trainings- oder Verbesserungszwecken von KI-Modellen

Anbieter: Clerk, Inc.

Verarbeitungsvorgang: Authentifizierung und Sitzungsmanagement

Ort der Verarbeitung: USA

Art der Daten: Login- und Metadaten
Datenschutzrechtliche Grundlage: EU-US Data Privacy Framework (DPF) oder Standarddatenschutzklauseln (Modul 3), Data Processing Addendum (DPA)

Besondere Einschränkungen: Keine Verarbeitung von Kommunikations- oder Inhaltsdaten

Anbieter: Meta Platforms Ireland Ltd. (WhatsApp Business API)

Verarbeitungsvorgang: Nachrichtentransport über externe Kommunikationskanäle **Ort der Verarbeitung:** EU und Drittland gemäß der Infrastruktur von Meta
Art der Daten: Kommunikationsdaten

Datenschutzrechtliche Grundlage: Auftragsverarbeitungsvertrag (AVV), Standarddatenschutzklauseln (SCC) **Besondere Einschränkungen:** Nutzung ausschließlich auf aktive Konfiguration und Auswahl durch den Auftraggeber

Anbieter: DATEV eG

Verarbeitungsvorgang: Buchhaltungs- und Schnittstellenverarbeitung

Ort der Verarbeitung: Deutschland (EU)

Art der Daten: Stamm- und Abrechnungsdaten

Datenschutzrechtliche Grundlage: Auftragsverarbeitungsvertrag (AVV), DATEV-Schnittstellenbedingungen **Besondere Einschränkungen:** Verarbeitung ausschließlich innerhalb der Europäischen Union

Anbieter: Cloudflare, Inc.

Verarbeitungsvorgang: DNS-Dienste, Content Delivery Network (CDN), Sicherheitsfunktionen **Ort der Verarbeitung:** Globales Edge-Netzwerk; Zugriff aus Drittstaaten technisch möglich **Art der Daten:** IP-Adressen und technische Metadaten

Datenschutzrechtliche Grundlage: EU-US Data Privacy Framework (DPF) oder Standarddatenschutzklauseln (Modul 3), Data Processing Addendum (DPA)

Besondere Einschränkungen: Kein Zugriff auf Kommunikations- oder Inhaltsdaten

Anbieter: Resend Labs, Inc.

Verarbeitungsvorgang: Transaktionaler E-Mail-Versand

Ort der Verarbeitung: USA

Art der Daten: Kommunikations-Metadaten

Datenschutzrechtliche Grundlage: EU-US Data Privacy Framework (DPF) oder Standarddatenschutzklauseln (Modul 3), Data Processing Addendum (DPA)

Besondere Einschränkungen: Keine dauerhafte Speicherung von Kommunikationsinhalten Ort, Datum Unterschrift

Interessent	**P-CATION Consulting and Solutions GmbH**
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Vorname, Nachname	Vorname, Nachname
_____	_____
Funktion	Funktion
_____	_____
Unterschrift	Unterschrift