AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Verarbeitung sind Anlage 1 zu entnehmen. Der tatsächliche Verarbeitungsumfang bestimmt sich nach den konkret beauftragten und erbrachten Leistungen. Die in Anlage 1 aufgeführten Leistungen und Datenkategorien definieren den maximal zulässigen Rahmen der Datenverarbeitung. Eine Erweiterung der Leistungen innerhalb dieses Rahmens bedarf keiner Vertragsänderung.

1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet grundsätzlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Abweichungen hiervon (Drittlandtransfer) sind nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und im Rahmen der in Anlage 3 dieses Vertrags aufgeführten Subunternehmer und Übermittlungstatbestände zulässig; weitergehende Drittlandverarbeitungen bedürfen der vorherigen Zustimmung des Auftraggebers.

1.4 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

1.5 Der konkrete Umfang der Datenverarbeitung je Auftrag wird durch die Beauftragung der Leistung (z.B. durch Serviceticket, E-Mail-Auftrag, mündliche Beauftragung) konkretisiert. Der Auftragsverarbeiter dokumentiert die erbrachten Leistungen in geeigneter Form (z.B. Ticketsystem, Serviceberichte). Diese Dokumentation dient als Nachweis des tatsächlichen Verarbeitungsumfangs.

2. Vertragslaufzeit und Kündigung

2.1 Der vorliegende Vertrag ist akzessorisch zum jeweiligen Hauptvertrag (insbesondere Dienst-, Werk-, Service- oder Softwareüberlassungsvertrag) zwischen den Parteien und teilt dessen Schicksal. Er beginnt mit Aufnahme der Datenverarbeitung im Auftrag und endet automatisch mit der Beendigung des Hauptvertrags, ohne dass es einer gesonderten Kündigung bedarf.

2.2 Eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen, solange der Hauptvertrag besteht und eine Verarbeitung personenbezogener Daten im Auftrag stattfindet. Die Kündigungsfristen und -modalitäten richten sich nach dem Hauptvertrag bzw. den zugrundeliegenden AGB der Berz Systems GmbH.

2.3 Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragsverarbeiter wesentliche Pflichten dieses Vertrags trotz

Abmahnung nicht einhält oder eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt und der Auftraggeber an dieser festhält.

2.4 Die Pflichten des Auftragsverarbeiters zur Rückgabe, Löschung und sicheren Vernichtung der vertragsgegenständlichen Daten (vgl. Ziff. 10) sowie weitere ihrer Natur nach nachwirkende Pflichten (insb. Verschwiegenheit, Mitwirkung bei behördlichen Anfragen) bleiben über die Vertragsbeendigung hinaus bestehen.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten. Der Auftragsverarbeiter ist nur berechtigt, eine Weisung nicht auszuführen, soweit er der Auffassung ist, dass die Weisung gegen anwendbare datenschutzrechtliche Vorschriften verstößt. In diesem Fall informiert der Auftragsverarbeiter den Auftraggeber unverzüglich (vgl. Art. 28 Abs. 3 und Art. 29 DSGVO).

3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.1a Kontrollen und Auskünfte erfolgen unter Beachtung der Vertraulichkeit sowie des Schutzes von Geschäftsgeheimnissen und der Rechte Dritter. Der Auftraggeber ist nicht berechtigt, im Rahmen von Kontrollen Einsicht in personenbezogene Daten oder Systeme anderer Auftraggeber/Mandanten des Auftragsverarbeiters zu nehmen. Soweit zur Erreichung des Kontrollzwecks erforderlich, kann der Auftragsverarbeiter geeignete Maßnahmen treffen, um eine Einsichtnahme in Daten anderer Mandanten auszuschließen (z.B. Schwärzungen, Einsichtnahme in Nachweise, Protokolle, System- und Konfigurationsauszüge, getrennte Testumgebungen).

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.3 Der Auftragsverarbeiter ist gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet (Art. 37 DSGVO i.V.m. § 38 BDSG), da die hierfür maßgeblichen Schwellenwerte (insb. weniger als 20 ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigte Personen) nicht erreicht werden und keine Verarbeitungen vorgenommen werden, die eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erfordern. Der Auftragsverarbeiter benennt stattdessen folgenden zentralen Ansprechpartner für den Datenschutz:

Name: Paul Berz
Email: datenschutz@berz.systems

Sollte der Auftragsverarbeiter zu einem späteren Zeitpunkt zur Bestellung eines Datenschutzbeauftragten verpflichtet sein oder freiwillig einen solchen bestellen, wird der Auftraggeber hierüber unverzüglich informiert. Änderungen über Person und / oder Kontaktdaten des Ansprechpartners für den Datenschutz sind dem Auftraggeber ebenfalls mitzuteilen.

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer ist unter folgenden Voraussetzungen gestattet:

a) Die Verarbeitung erfolgt an einem Ort, der ein dem Betriebsstandort vergleichbares Schutzniveau gewährleistet (insbesondere Homeoffice, Co-Working-Spaces oder mobiles Arbeiten im Inland sowie im europäischen Wirtschaftsraum).
b) Der Auftragsverarbeiter stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten auch außerhalb der Betriebsstätte gewahrt bleibt. Hierzu zählen insbesondere: verschlüsselte Datenübertragung (z.B. VPN), Bildschirmsperre, Zugriffsbeschränkungen, Verhinderung der Einsichtnahme durch Dritte sowie sichere Aufbewahrung von Arbeitsmitteln.
c) Eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und ist nur unter Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO zulässig.
d) Der Auftragsverarbeiter dokumentiert die getroffenen Schutzmaßnahmen und legt diese dem Auftraggeber auf Anfrage vor.

5.5 Der Auftragsverarbeiter hat zu gewährleisten, 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). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

5.7 **Einsatz von KI-gestützten und agentischen Systemen**

5.7.1 Der Auftragsverarbeiter ist berechtigt, zur Erbringung der vereinbarten Leistungen generative KI-Systeme (insbesondere Large Language Models) und agentische Workflows (autonom handelnde Software-Agenten mit kontrolliertem Tool-Zugriff, z.B. via Model Context Protocol / MCP) einzusetzen. Die konkreten Anwendungsbereiche, eingesetzten Anbieter, Autonomiegrade und Schutzmaßnahmen ergeben sich aus Anlage 1 (Auftragsdetails) und Anlage 3 (Subunternehmer).

5.7.2 KI-Inferenz, bei der personenbezogene Daten des Auftraggebers in den Prompt-Kontext oder als Eingabe in Tool-Aufrufe gelangen, erfolgt ausschließlich über Endpunkte innerhalb der Europäischen Union bzw. innerhalb der „EU Data Boundary“ der eingesetzten Anbieter (insb. AWS Bedrock EU-Region, Google Vertex AI EU-Regionen, Azure OpenAI EU Data Boundary, Mistral AI/Scaleway/OVH EU). Eine Nutzung von Direkt-APIs außerhalb der EU (z.B. anthropic.com, openai.com, api.gemini.google) für personenbezogene Daten des Auftraggebers findet nicht statt.

5.7.3 Eine Verwendung der vertragsgegenständlichen Daten zum Training von KI-Modellen ist ausgeschlossen. Soweit vom jeweiligen Anbieter angeboten, wird eine Zero-Retention-Konfiguration aktiviert. Modellanbieter (einschließlich der via Bedrock, Vertex AI Model Garden oder vergleichbarer Plattformen bereitgestellten Anbieter) erhalten keinen eigenständigen Zugriff auf die vertragsgegenständlichen Daten; die Inferenz erfolgt innerhalb der Infrastruktur des jeweiligen Hyperscalers in der EU.

5.7.4 **Zulässige Autonomie:** Der Auftragsverarbeiter darf KI- und Agentensysteme in allen Autonomiegraden gemäß Anlage 1 einsetzen, einschließlich autonomer Ausführung schreibender Operationen („Stufe 4/5“), soweit dies der Erbringung der beauftragten Leistung dient und die in Anlage 1 vorgesehenen Schutzmaßnahmen (Audit-Logging, Least-Privilege, Mengenbegrenzung, Notfall-Stopp, Reversibilitäts-Prüfung) eingehalten werden. Eine zwingende menschliche Freigabe (Human-in-the-Loop) im Einzelfall besteht nur, soweit dies in Anlage 1 für den jeweiligen Autonomiegrad (insb. Stufe 3 sowie die Eskalations-Trigger in Stufe 5) vorgesehen ist oder eine Weisung des Auftraggebers dies anordnet.

5.7.5 **Ausschlüsse und Schutzpflichten:** Der Auftragsverarbeiter wird KI-/Agentensysteme nicht einsetzen für

a) automatisierte Einzelentscheidungen, die gegenüber Betroffenen rechtliche Wirkung entfalten oder sie in ähnlich erheblicher Weise beeinträchtigen (Art. 22 DSGVO), es sei denn, der Auftraggeber weist dies ausdrücklich an und stellt seinerseits die gesetzlichen Schutzmaßnahmen sicher;
b) die Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO;
c) Profilbildung, Beobachtung oder Bewertung natürlicher Personen, soweit nicht ausdrücklich beauftragt;
d) Maßnahmen, die unter Anhang III der Verordnung (EU) 2024/1689 (KI-Verordnung) als Hochrisiko-KI-Systeme einzustufen wären, ohne dass die dafür vorgesehenen Anforderungen erfüllt sind;
e) Praktiken, die nach Art. 5 der Verordnung (EU) 2024/1689 verboten sind (insbesondere unterschwellige Beeinflussung natürlicher Personen, Ausnutzung von Schwächen oder Schutzbedürftigkeit, Social Scoring, biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum).

5.7.6 **Transparenz und Weisungsrecht:** Das Weisungsrecht des Auftraggebers nach Ziff. 3 erstreckt sich ausdrücklich auch auf Art, Umfang, Autonomiegrad und Konfiguration der eingesetzten KI- und Agentensysteme. Der Auftraggeber kann insbesondere

a) den Einsatz von KI-/Agentensystemen für einzelne Workflows oder Datenkategorien einschränken oder ausschließen,
b) eine menschliche Freigabe (Human-in-the-Loop) für bestimmte Workflows anordnen,
c) Einsicht in Audit-Logs, Tool-Definitionen und Guardrail-Konfigurationen verlangen.

Wesentliche Änderungen am eingesetzten KI-Stack (neue Modellanbieter, neue Autonomiegrade in produktiven Kundensystemen, neue Tool-Integrationen mit personenbezogenen Daten) werden dem Auftraggeber entsprechend der Subunternehmer-Änderungsregelung nach Ziff. 8.1 mitgeteilt.

5.7.7 **Klarstellung – Tätigkeiten ohne Verarbeitung personenbezogener Daten:**

5.7.7.1 Tätigkeiten des Auftragsverarbeiters, bei denen **keine** personenbezogenen Daten des Auftraggebers verarbeitet werden – insbesondere allgemeine Software-Entwicklung, Architektur- und Konzeptarbeit, Erstellung generischer Boilerplate- und Bibliotheks-Codes, Refactoring oder Erstellung von Tests auf Basis nicht-personenbezogener Code-Bestandteile, Recherche auf Basis öffentlich zugänglicher Dokumentation – stellen keine Auftragsverarbeitung im Sinne des Art. 28 DSGVO dar. Für solche Tätigkeiten gelten die Beschränkungen der Ziff. 5.7.2 (EU-only Inferenz) nicht; der Auftragsverarbeiter darf dafür auch Direkt-APIs von KI-Anbietern außerhalb der EU einsetzen (z.B. Anthropic, OpenAI, Google AI Studio).

5.7.7.2 Der Auftragsverarbeiter stellt durch geeignete organisatorische Maßnahmen sicher, dass im Rahmen der Tätigkeiten nach Ziff. 5.7.7.1 keine personenbezogenen Daten des Auftraggebers in die Direkt-APIs gelangen. Dies umfasst insbesondere:

a) Verzicht auf das Einfügen von Produktiv-Logs, Stack-Traces, Test-Fixtures, Konfigurationsdateien oder Datenbankauszügen mit personenbezogenen Daten in den Prompt-Kontext;
b) Pseudonymisierung oder Entfernung personenbezogener Daten aus übergebenen Artefakten, soweit deren Einbindung technisch erforderlich ist;
c) Vorrangiger Einsatz von EU-Endpunkten (insb. AWS Bedrock, Vertex AI), sobald nicht zweifelsfrei ausgeschlossen werden kann, dass personenbezogene Daten betroffen sind.

5.7.7.3 Für Direkt-APIs nach Ziff. 5.7.7.1 stellt der Auftragsverarbeiter zudem sicher, dass mit dem jeweiligen Anbieter (a) ein Data Processing Addendum bzw. eine vergleichbare vertragliche Grundlage besteht, (b) die Nutzung der übermittelten Daten für das Modelltraining ausgeschlossen ist und (c) eine Zero-Retention- bzw. No-Logging-Konfiguration aktiviert ist, soweit anbieterseitig verfügbar.

5.7.7.4 Vertraulichkeitspflichten des Auftragsverarbeiters bezüglich nicht-personenbezogener, aber gleichwohl vertraulicher Informationen des Auftraggebers (z.B. Geschäftsgeheimnisse, Quellcode, Architekturentscheidungen) bleiben unberührt und richten sich nach dem Hauptvertrag bzw. den AGB.

5.7.8 **Transparenzpflicht nach Art. 50 KI-Verordnung:** Soweit der Auftragsverarbeiter KI-Systeme einsetzt, die unmittelbar mit natürlichen Personen interagieren (insbesondere automatisierte Antworten auf Tickets, E-Mails oder Chat-Nachrichten gegenüber Mitarbeitern des Auftraggebers oder dessen Kunden), wird er sicherstellen, dass die betroffenen Personen darüber informiert werden, dass sie mit einem KI-System interagieren bzw. Inhalte erhalten, die mit Unterstützung eines KI-Systems erstellt wurden (Art. 50 Abs. 1 und Abs. 4 der Verordnung (EU) 2024/1689). Die Hinweispflicht entfällt, soweit sich der Einsatz aus den Umständen offensichtlich ergibt oder gesetzliche Ausnahmen greifen. Der Hinweis kann in geeigneter Form erfolgen, insbesondere durch entsprechende Kennzeichnung in der Antwort selbst, in der Signatur oder im Antwortkanal.

5.7.9 **KI-Kompetenz nach Art. 4 KI-Verordnung:** Der Auftragsverarbeiter stellt sicher, dass die mit dem Einsatz von KI-Systemen befassten Personen über ein ausreichendes Maß an KI-Kompetenz im Sinne des Art. 4 der Verordnung (EU) 2024/1689 verfügen. Maßnahmen zur Aufrechterhaltung dieser Kompetenz (insbesondere fortlaufende Fortbildung, Auswertung von Anbieter-Dokumentationen, interne Auswertung von Vorfällen und Audit-Logs) werden in geeigneter Weise dokumentiert und sind dem Auftraggeber auf Verlangen vorzulegen.

5.7.10 **Rollen und Pflichten nach der KI-Verordnung:**

Der Auftragsverarbeiter ist beim Einsatz der in Anlage 3 aufgeführten KI-Systeme in der Regel **Betreiber** im Sinne von Art. 3 Nr. 4 der Verordnung (EU) 2024/1689, nicht Anbieter. Er bringt keine KI-Systeme eigenständig auf den Markt und übernimmt keine Anbieterpflichten (insb. Konformitätsbewertung, CE-Kennzeichnung, Eintragung in die EU-Datenbank).

Der Auftragsverarbeiter setzt ausschließlich KI-Systeme und GPAI-Modelle (Art. 3 Nr. 63 KI-Verordnung) ein, deren Anbieter die Anforderungen der KI-Verordnung erfüllen und für die eine geeignete vertragliche Grundlage (DPA, AUP) besteht. Die in Anlage 3 aufgeführten KI-Anbieter (insb. AWS Bedrock, Azure OpenAI, Google Vertex AI, Mistral AI, Scaleway) sind anhand dieser Anforderungen ausgewählt.

Weist der Auftraggeber den Einsatz eines Hochrisiko-KI-Systems im Sinne des Anhangs III der KI-Verordnung an, informiert der Auftragsverarbeiter den Auftraggeber über die daraus entstehenden Betreiberpflichten nach Art. 26 KI-Verordnung (u. a. Grundrechte-Folgenabschätzung, Protokollierung, menschliche Beaufsichtigung, Mitarbeiterinformation). Die Umsetzung einer solchen Beauftragung bedarf einer ergänzenden schriftlichen Vereinbarung.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer oder den Wechsel bestehender Subunternehmer, informiert er den Auftraggeber hierüber vorab in schriftlicher oder elektronischer Form (z.B. per E-Mail). Die Zustimmung des Auftraggebers gilt als

erteilt, wenn er der Änderung nicht innerhalb einer Frist von 2 Wochen nach Zugang der Information schriftlich oder in elektronischer Form widerspricht. Im Falle eines berechtigten Widerspruchs ist der Auftragsverarbeiter berechtigt, den Vertrag aus wichtigem Grund zu kündigen, sofern die Leistungserbringung ohne den betreffenden Subunternehmer nicht zumutbar ist.

8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können.

8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.

8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.1a Der Auftragsverarbeiter informiert den Auftraggeber über Verletzungen des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) unverzüglich nach Bekanntwerden.

9.1b Bei schwerwiegenden Vorfällen mit KI-Systemen im Sinne von Art. 3 Nr. 49 der Verordnung (EU) 2024/1689 – insbesondere bei Vorfällen, die zu einem Risiko für Gesundheit, Sicherheit oder Grundrechte natürlicher Personen führen oder geführt haben – informiert der Auftragsverarbeiter den Auftraggeber unverzüglich. Etwaige Meldepflichten gegenüber Marktüberwachungsbehörden nach Art. 73 der Verordnung (EU) 2024/1689 bleiben davon unberührt.

9.1c Die Meldung kann initial in Textform (z.B. E-Mail) oder telefonisch erfolgen; bei telefonischer Erstmeldung wird der Auftragsverarbeiter die wesentlichen Informationen unverzüglich in Textform nachreichen. Die Erstmeldung enthält – soweit zu diesem Zeitpunkt verfügbar – mindestens:

a) eine Beschreibung der Art des Vorfalls (inkl. betroffene Systeme),
b) Kategorien der betroffenen personenbezogenen Daten und betroffenen Personen,
c) eine grobe Einschätzung des Umfangs (z.B. Anzahl Datensätze/Betroffene),
d) die wahrscheinlichen Folgen des Vorfalls,
e) bereits ergriffene bzw. geplante Abhilfemaßnahmen,
f) eine Kontaktstelle für Rückfragen.

9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu

löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

Die Rückgabe bzw. Löschung erfolgt, soweit nicht abweichend vereinbart, spätestens innerhalb von 30 Tagen nach Vertragsbeendigung. Sofern eine Rückgabe verlangt wird, erfolgt diese in einem gängigen, maschinenlesbaren Format oder in dem Format, in dem die Daten dem Auftragsverarbeiter bereitgestellt wurden, soweit technisch möglich und zumutbar.

Soweit personenbezogene Daten in Datensicherungen (Backups) oder Wiederherstellungspunkten enthalten sind, werden diese im Rahmen der regulären Backup-Retention gelöscht bzw. überschrieben. Bis zur endgültigen Löschung werden solche Backup-Daten gesperrt und nicht produktiv verarbeitet; ein Zugriff erfolgt nur, soweit dies zur Wiederherstellung der Systeme erforderlich ist.

Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

12.5 Für die Haftung des Auftragsverarbeiters unter diesem Vertrag gelten die Haftungsregelungen und -beschränkungen des Hauptvertrags bzw. der Allgemeinen Geschäftsbedingungen (AGB)

entsprechend, soweit dies gesetzlich zulässig ist. Eine über den Hauptvertrag hinausgehende Haftung wird – vorbehaltlich zwingender gesetzlicher Vorschriften – nicht begründet.

12.6 Soweit die Europäische Kommission oder zuständige nationale Behörden im Rahmen der Durchführung der Verordnung (EU) 2024/1689 (KI-Verordnung) – insbesondere durch Codes of Practice, delegierte Rechtsakte oder Leitlinien zu GPAI-Modellen und Betreiberpflichten – neue Anforderungen veröffentlichen, passen die Parteien die einschlägigen Regelungen dieses Vertrags (insb. Ziff. 5.7 und Anlage 3) im gegenseitigen Einvernehmen an. Der Auftragsverarbeiter informiert den Auftraggeber über wesentliche neue Anforderungen, die die vertragsgegenständlichen KI-Systeme betreffen.

Anlage 1 – Auftragsdetails

1. Der vorliegende Vertrag umfasst folgende Leistungen:

Technischer Support und Wartung:

- Administration und Wartung von Server-Infrastrukturen (On-Premise und Cloud)
- Fernwartung und Remote-Support für Arbeitsplätze und Systeme
- Installation, Konfiguration und Updates von Betriebssystemen und Anwendungssoftware
- Monitoring und Überwachung von IT-Systemen
- Fehlerdiagnose und -behebung an Hard- und Software

Netzwerk und Sicherheit:

- Einrichtung und Verwaltung von Firewalls, VPN-Verbindungen und Netzwerkkomponenten
- Administration von Backup- und Disaster-Recovery-Lösungen
- Durchführung von Sicherheitsupdates und Patch-Management
- Virenschutz- und Anti-Malware-Dienste
- Verwaltung von Zugriffsrechten und Authentifizierungssystemen

Cloud Services:

- Bereitstellung und Administration von Cloud Lösungen (SaaS)
- Verwaltung von Cloud-Plattformen
- Migration von Daten in Cloud-Umgebungen
- Hosting und Betrieb von Anwendungen und Datenbanken

Benutzerverwaltung:

- Einrichtung und Verwaltung von Benutzerkonten und E-Mail-Postfächern
- Administration von Active Directory oder vergleichbaren Verzeichnisdiensten
- Rechteverwaltung für Datei- und Ordnerzugriffe
- Schulung von Mitarbeitern im Umgang mit IT-Systemen

Hardware und Datenmanagement:

- Beschaffung, Lieferung und Installation von Hardware (PCs, Notebooks, Server, Netzwerkgeräte)
- Datenmigration bei Systemwechseln oder Hardwareaustausch
- Sichere Datenvernichtung alter Hardware
- Inventarisierung und Asset-Management

Spezielle Dienste:

- Einrichtung und Betrieb von Ticketsystemen und Help-Desk-Lösungen
- Verwaltung von CRM- oder ERP-Systemen
- Archivierungslösungen für E-Mails und Dokumente
- Telefonie- und Unified-Communications-Lösungen

KI-gestützte Verarbeitung (Generative AI / agentische Workflows):

Anwendungsbereiche (Zweck):

- KI-gestützte Auswertung, Analyse und Klassifikation von Support-Tickets, Kundenanfragen, E-Mail-Kommunikation und Telefonprotokollen

- KI-gestützte Auswertung von System-Logs, Telemetrie-, Monitoring- und Tracing-Daten zur Fehleranalyse, Performance-Optimierung und Incident-Response
- KI-gestützte Analyse von Konfigurationsdateien, Skripten, Infrastruktur-as-Code und Code-Fragmenten im Rahmen von Wartung, Hardening, Migration und DevOps
- KI-gestützte Erstellung von Dokumentation, Reports, Antwortentwürfen, Code, Tests und Migrationsskripten
- Agentische Workflows: autonom oder semi-autonom handelnde Software-Agenten mit kontrolliertem Tool-Zugriff (z.B. via Model Context Protocol / MCP, Function-Calling, Plugin-APIs) auf Drittsysteme – insbesondere Ticket- und CRM-Systeme, Monitoring- und Logging-Plattformen, Versionskontrolle (Git), Build-/Deploy-Pipelines, Cloud-Management-APIs und ERP- bzw. Buchhaltungssysteme – im Rahmen der jeweils beauftragten Leistung

Autonomiegrade: Der Auftragsverarbeiter setzt KI-Systeme in verschiedenen Autonomiegraden ein. Welcher Grad jeweils zur Anwendung kommt, richtet sich nach Risikoprofil, Reversibilität und Schadenspotenzial der jeweiligen Operation. Der Auftraggeber kann den Autonomiegrad nach Ziff. 5.7.6 per Weisung einschränken.

- **Stufe 1 – Read/Analyze:** rein lesende Analyse, Klassifizierung und Empfehlung ohne Schreibvorgänge in Kundensysteme.
- **Stufe 2 – Draft/Suggest:** Erzeugung von Entwürfen, Vorschlägen, Antwortbausteinen, Pull-Requests; Übernahme erfolgt durch Menschen.
- **Stufe 3 – Assist mit Freigabe:** die KI bereitet Aktionen vor; ein Mensch bestätigt vor Wirksamwerden („Human-in-the-Loop“).
- **Stufe 4 – Autonom (unkritisch/reversibel):** eigenständige Ausführung in unkritischen oder vollständig reversiblen Bereichen, z.B. Ticket-Klassifikation, automatische Antworten innerhalb klar definierter Themenfelder, interne Dokumentationspflege, Test- und Staging-Pipelines, Routing- und Tagging-Operationen, Erstellung von Angebots-/Rechnungsentwürfen ohne automatischen Versand.
- **Stufe 5 – Autonom (produktiv):** eigenständige Ausführung in produktiven Kundensystemen ausschließlich innerhalb vorab definierter Guardrails – technisch eingeschränkter Tool-Scope, Mengen- und Frequenzlimits, automatische Anomalieerkennung mit Rollback, lückenloses Audit-Logging. Stufe 5 setzt eine dokumentierte Risikobewertung pro Workflow voraus.

Technische und organisatorische Schutzmaßnahmen:

- **EU-only Inferenz für personenbezogene Daten:** sobald personenbezogene Daten des Auftraggebers in den Prompt-Kontext, in Tool-Aufrufe oder in Trainingseingaben gelangen können, erfolgt die Inferenz ausschließlich auf Endpunkten innerhalb der EU bzw. der EU Data Boundary der eingesetzten Anbieter (insb. AWS Bedrock eu-central-1, Google Vertex AI in EU-Regionen, Azure OpenAI EU Data Boundary, Mistral AI/Scaleway/OVH EU). Eine Nutzung von Direkt-APIs außerhalb der EU (z.B. anthropic.com, openai.com, api.gemini.google) für personenbezogene Daten des Auftraggebers findet nicht statt. Die Zulässigkeit der Nutzung solcher Direkt-APIs für rein technische, PII-freie Tätigkeiten bleibt von Ziff. 5.7.7 unberührt.
- **Kein Training, Zero-Retention:** keine Nutzung der vertragsgegenständlichen Daten für das Training von KI-Modellen (Opt-out bzw. vertraglicher Ausschluss); Zero-Retention-Konfiguration soweit vom jeweiligen Anbieter angeboten.
- **Audit-Logging:** lückenlose Protokollierung sämtlicher Tool-Aufrufe agentischer Workflows (Zeitstempel, ausführender Agent/Identität, aufgerufenes Tool, Parameter, Ergebnis bzw. Statuscode);

Protokolle werden manipulationssicher gespeichert und stehen dem Auftraggeber auf Verlangen zur Verfügung.

- **Least-Privilege & Sandboxing:** technische Beschränkung des Tool-Scopes auf das jeweils erforderliche Mindestmaß; getrennte Identitäten/API-Keys pro Workflow; Sandbox-/Staging-Umgebungen für die Erprobung neuer agentischer Workflows.
- **Mengen- und Frequenzbegrenzungen:** Rate-Limits und Maximalmengen für schreibende Operationen, automatische Eskalation an einen Menschen bei Überschreiten der Schwellenwerte.
- **Notfall-Stopp:** jederzeitige Möglichkeit, einzelne Workflows oder den gesamten KI-/Agentenbetrieb manuell oder regelbasiert anzuhalten („Kill Switch").
- **Reversibilität:** bevorzugter Einsatz reversibler Operationen; bei irreversiblen oder mengenmäßig erheblichen Operationen Eskalation auf Stufe 3 (Freigabe durch Menschen).
- **Modell- und Prompt-Hardening:** Verwendung von Systemprompts/Guardrails zur Vermeidung von Prompt-Injection-Effekten; periodische Überprüfung und Aktualisierung der Guardrails.

Ausschlüsse:

- Keine automatisierten Einzelfallentscheidungen i.S.d. Art. 22 DSGVO ohne ausdrückliche Weisung des Auftraggebers und ergänzende Schutzmaßnahmen.
- Keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO durch KI-Systeme.
- Kein Einsatz für Hochrisiko-KI-Anwendungen i.S.d. Anhangs III der Verordnung (EU) 2024/1689 ohne Erfüllung der dafür vorgesehenen Anforderungen.
- Keine Nutzung von KI-Systemen für Maßnahmen der Beweissicherung, Beobachtung oder Profilbildung gegenüber natürlichen Personen, soweit nicht ausdrücklich beauftragt.

Transparenz: Wesentliche Änderungen am eingesetzten KI-Stack (neue Modellanbieter, neue Tool-Integrationen mit personenbezogenen Daten, Anhebung des Autonomiegrades in produktiven Kundensystemen) werden dem Auftraggeber gemäß Ziff. 8.1 mitgeteilt. Das Weisungsrecht des Auftraggebers nach Ziff. 5.7.6 bleibt unberührt.

2. Datenarten – Umfang und Rahmen der Verarbeitung

Wichtiger Hinweis zum Verarbeitungsumfang: Die nachfolgende Auflistung definiert den **maximalen Rahmen** der möglichen Datenverarbeitung. Der tatsächliche Verarbeitungsumfang richtet sich ausschließlich nach den konkret beauftragten Leistungen.

Grundsatz: Je nach Auftrag verarbeiten wir nur die für die beauftragte Leistung jeweils erforderlichen Daten aus den nachfolgend aufgeführten Kategorien. Nicht beauftragte Leistungen führen nicht zur Verarbeitung der entsprechenden Datenkategorien.

Erweiterungen: Der Verarbeitungsumfang kann im Serviceverlauf erweitert werden, sofern die Erweiterung innerhalb des hier definierten Rahmens erfolgt. Eine Vertragsanpassung ist in diesem Fall nicht erforderlich.

Besonderheit bei Wartung und Support: Soweit Gegenstand des Auftrags reine **Wartungs-, Administrations- oder Supportleistungen** sind, ist die Verarbeitung personenbezogener Daten nicht Hauptzweck, sondern lediglich eine technisch notwendige Nebenfolge. Der Auftragsverarbeiter beschränkt den Zugriff auf Daten in diesen Fällen auf das zur Erbringung der geschuldeten Leistung (z.B. Fehleranalyse) zwingend erforderliche Mindestmaß. Eine dauerhafte Speicherung, Kopie oder

anderweitige Nutzung der Daten findet – anders als bei Hosting-Leistungen – nicht statt, es sei denn, dies ist zur Fehlerbehebung temporär unumgänglich.

2a. Art der Verarbeitung / Verarbeitungsvorgänge

Je nach konkret beauftragter Leistung können insbesondere folgende Verarbeitungsvorgänge erforderlich sein. Der Auftragsverarbeiter beschränkt sich auf das jeweils erforderliche Mindestmaß:

- Zugriff/Einsichtnahme (z.B. Remote-Support, Administration, auch unbeaufsichtigt im Rahmen von Managed Services oder nach Vereinbarung)
- Erhebung/Entgegennahme von Daten (z.B. via Ticket, E-Mail, Telefonprotokoll)
- Speicherung/Hosting (insbesondere bei SaaS- und Hosting-Leistungen)
- Organisation, Strukturierung und Verwaltung (z.B. Benutzer-/Rechteverwaltung)
- Änderung/Berichtigung (z.B. Konfiguration, Datenpflege im Rahmen des Supports)
- Übermittlung/Weitergabe (z.B. an Subunternehmer, soweit erforderlich)
- Protokollierung/Logging (insbesondere zur IT-Sicherheit und Fehleranalyse)
- Wiederherstellung aus Backups/Disaster-Recovery (soweit vereinbart)
- Löschung/Verkürzung der Verfügbarkeit (z.B. im Rahmen von Retention-Konzepten)

Personenbezogene Stammdaten:

- Name, Vorname, Titel
- Geburtsdatum, Geburtsort
- Geschlecht
- Privatanschrift (Straße, Hausnummer, PLZ, Ort, Land)
- Geschäftsanschrift
- Personalausweis- oder Reisepassnummer
- Staatsangehörigkeit

Kontaktdaten:

- Telefonnummern (Festnetz, Mobil)
- E-Mail-Adressen (privat und geschäftlich)
- Fax-Nummern
- Messenger-Kontakte (Skype, Teams, etc.)

Beschäftigungsdaten:

- Mitarbeiternummer, Personalnummer
- Abteilung, Kostenstelle
- Position, Funktion, Berufsbezeichnung
- Vorgesetzter
- Eintrittsdatum, Beschäftigungsdauer
- Arbeitszeiten, Arbeitszeitmodelle
- Urlaubsdaten, Abwesenheiten

Vertragsdaten:

- Vertragsunterlagen
- Kundennummern, Lieferantennummern
- Auftrags- und Rechnungsdaten
- Zahlungsinformationen
- Bonitätsdaten

Finanz- und Bankdaten:
- Bankverbindung (IBAN, BIC, Kontonummer, Bankleitzahl)
- Kreditkartendaten
- Steuer-Identifikationsnummer
- Umsatzsteuer-ID
- Gehaltsdaten, Lohnabrechnungen

IT-Nutzungsdaten:
- Benutzernamen, Benutzer-IDs
- Passwörter (verschlüsselt)
- IP-Adressen (statisch und dynamisch)
- MAC-Adressen
- Computer-Namen, Geräte-IDs
- Zugriffsberechtigungen und Rollen
- Log-Dateien, Protokolldaten
- Zeitstempel von Systemzugriffen

Kommunikationsdaten:
- E-Mail-Inhalte und -Metadaten (Absender, Empfänger, Betreff, Datum)
- Anhänge von E-Mails
- Chat-Verläufe, Messenger-Nachrichten
- Telefonverbindungsdaten
- Kalenderdaten, Termineinträge
- Aufgaben und Notizen

Datei- und Dokumentendaten:
- Textdokumente, Tabellen, Präsentationen
- PDF-Dokumente
- Bilder, Fotos, Videos
- Dateimetadaten (Autor, Erstellungsdatum, Änderungsdatum)
- Versionsstände von Dokumenten

Standort- und Bewegungsdaten:
- Geodaten bei mobilen Endgeräten
- Zutrittsprotokolle
- VPN-Verbindungsprotokolle

Sonstige Daten:
- Führerscheindaten (bei Fuhrparkverwaltung)
- Kfz-Kennzeichen
- Sozialversicherungsnummern
- Bewerbungsunterlagen (Lebenslauf, Zeugnisse, Fotos)
- Kundenbewertungen, Feedback
- Notfallkontakte
- Versicherungsdaten

Technische Metadaten:
- Browser-Informationen, User-Agent-Strings

- Betriebssystem-Versionen
- Cookie-Daten
- Session-IDs
- Netzwerkverkehrsdaten
- Performance- und Diagnosedaten

3. Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um Mitarbeiter und Beschäftigte des Auftraggebers:
- Angestellte (Vollzeit, Teilzeit, geringfügig Beschäftigte)
- Führungskräfte, Geschäftsführung, Vorstand
- Auszubildende, Praktikanten, Werkstudenten
- Freie Mitarbeiter, Freelancer
- Leiharbeitnehmer
- Ehemalige Mitarbeiter
- Bewerber

Geschäftspartner:
- Kunden und Interessenten
- Lieferanten und Dienstleister
- Vertriebspartner, Handelsvertreter
- Kooperationspartner
- Berater, externe Sachverständige

Kontaktpersonen bei Geschäftspartnern:
- Ansprechpartner bei Kundenunternehmen
- Verantwortliche bei Lieferanten
- Entscheidungsträger in Partnerorganisationen

Besucher und externe Personen:
- Besucher der Geschäftsräume
- Teilnehmer an Veranstaltungen, Schulungen, Webinaren
- Messekontakte

Endkunden und Verbraucher:
- Privatkunden
- Online-Shop-Kunden
- Newsletter-Abonnenten
- Website-Besucher

Weitere betroffene Personen:
- Angehörige von Mitarbeitern (z.B. bei Notfallkontakten)
- Bevollmächtigte und gesetzliche Vertreter
- Patienten (bei Gesundheitseinrichtungen)
- Schüler, Studenten (bei Bildungseinrichtungen)
- Vereinsmitglieder (bei Vereinen und Verbänden)
- Bürger, Antragsteller (bei Behörden und öffentlichen Stellen)
- Vertragspartner bei privatrechtlichen Verträgen

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

Mandantentrennung auf Organisationsebene:

- In allen eingesetzten Systemen erfolgt eine strikte Zuordnung der Daten zum jeweiligen Kunden/Auftraggeber durch Unternehmens-/Firmen-/Site-Strukturen
- Jeder Kunde erhält eine dedizierte Organisationseinheit (Ordner, Firma, Company, Site), unter der sämtliche zugehörigen Daten strukturiert werden

Zugriffskontrolle durch ACLs (Access Control Lists):

- Rollenbasierte Zugriffsrechte stellen sicher, dass nur autorisierte Mitarbeiter Zugriff auf kundenbezogene Daten erhalten
- In sensiblen Systemen werden Berechtigungen explizit pro Kunde/Organisationseinheit vergeben
- Dateiablagen sind durch ACLs auf Ordnerebene gegen unbefugten Zugriff geschützt

Dateisystembasierte Trennung:

- Dokumentationen und Dateiablagen verwenden jeweils einen separaten Ordner pro Kunde
- Strukturierte Ablage verhindert Vermischung von Kundendaten

Attributbasierte Zuordnung:

- Wo eine strukturelle Trennung technisch nicht möglich ist, erfolgt die Zuordnung über eindeutige Kundenattribute

Systemimmanente Zweckbindung:

- Alle Systeme sind so konfiguriert, dass eine systemübergreifende Vermischung von Kundendaten technisch ausgeschlossen ist

2. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

2.1 Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

Verschlüsselung bei der Übertragung (Transport):

- Sämtliche Kommunikation zwischen Clients und Servern erfolgt über verschlüsselte Verbindungen (TLS/SSL)
- Webbasierte Anwendungen sind ausschließlich über HTTPS erreichbar

- E-Mail-Übertragung erfolgt verschlüsselt (TLS)
- Administrative Zugriffe auf Systeme erfolgen über verschlüsselte Protokolle (SSH, RDP über VPN)

Verschlüsselung im Ruhezustand (Data at Rest):
- Festplattenvollverschlüsselung auf allen Servern und Arbeitsplatzrechnern
- Datenbanken werden auf verschlüsselten Volumes betrieben
- Dateiablagen (SMB-Shares) liegen auf verschlüsselten Speichersystemen
- Backups werden verschlüsselt gespeichert
- Passwortmanagement-Systeme nutzen zusätzliche End-to-End-Verschlüsselung

Mobile Datenträger und Endgeräte:
- Laptops und mobile Endgeräte sind mit Festplattenverschlüsselung ausgestattet
- Externe Datenträger werden bei Verwendung verschlüsselt

Netzwerksegmentierung und Systemtrennung Logische Netzwerktrennung:
- Einsatz von VLANs zur Segmentierung verschiedener Netzwerkbereiche
- Trennung von Produktiv-, Management- und DMZ netzen
- Firewall-Regeln zwischen den Segmenten zur Zugriffskontrolle

Virtualisierung und Isolation:
- Betrieb von Systemen in isolierten virtuellen Maschinen (VMs)
- Jede VM stellt eine eigenständige, abgeschottete Umgebung dar

2.2 Pseudonymisierung

Eingeschränkt. Eine vollständige Pseudonymisierung erfolgt in der Regel nicht, da die Verarbeitung personenbezogener Daten zum Zweck der Auftragserfüllung (z.B. IT-Support, Benutzerverwaltung) die Kenntnis der Identität der betroffenen Personen erfordert. Soweit technisch möglich und sinnvoll, wird hierbei jedoch das Prinzip der Datenminimierung beachtet.

2.3 Zutrittskontrolle

Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

Technische Gerätesicherung (primäre Schutzebene):
- Biometrische Zugangssperren an mobilen Endgeräten
- Passwortschutz aller Arbeitsgeräte nach BSI-Empfehlungen
- Vollverschlüsselung aller Festplatten und Datenträger (LUKS2, ZFS)
- Automatische Bildschirmsperre mit angemessenem Timeout
- Hardware-Tokens als Zwei-Faktor-Authentifizierung und für kryptographische Verbindungen (SSH)

Physische Sicherung der Arbeitsumgebungen:
- Homeoffice (Geschäftsführung): Videoüberwachung des Gebäudes (Eingang, Garten) sowie einbruchshemmende Fensterbeschläge am Standort der zentralen Aktenaufbewahrung
- Externe Arbeitsplätze: Keine Bearbeitung physischer Dokumente, digitale Arbeit erfolgt unter diskreten Bedingungen mit Sichtschutz
- Verschlossene Aufbewahrung von physischen Unterlagen im Homeoffice

Organisatorische Maßnahmen:
- Clean-Desk-Policy: Keine sensiblen Unterlagen offen liegen lassen

- Bildschirme sind bei Verlassen des Arbeitsplatzes gesperrt
- Mobile Arbeitsgeräte werden bei Abwesenheit und Transport sicher und verdeckt verwahrt

2.4 Zugangskontrolle

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

Benutzer- und Rechteverwaltung:
- Zuordnung von Benutzerrechten nach Rollen und Aufgaben
- Erstellen individueller Benutzerprofile
- Privilegierte Zugänge (z.B. Administratorkonten) werden nur von autorisierten Mitarbeitern genutzt und dokumentiert
- Zuordnung von Benutzerprofilen zu IT-Systemen mit Least-Privilege-Prinzip

Authentifizierung:
- Authentifikation mit Benutzername und Passwort
- Passwort-Richtlinien (Mindestlänge, Komplexität nach BSI-Empfehlung)
- Authentifikation mit biometrischen Verfahren (mobile Endgeräte)
- Multi-Faktor-Authentifizierung (Hardware-Tokens, TOTP) für kritische Systeme
- Mutual TLS (mTLS) bei sensiblen Anwendungen zur gegenseitigen Zertifikatsauthentifizierung
- Passwort-Manager für sichere Passwortverwahrung

Netzwerksicherheit:
- Einsatz von VPN-Technologie bei der Übertragung von Daten
- Einsatz einer Hardware-Firewall
- Einsatz von Software-Firewalls auf allen Endgeräten
- Netzwerksegmentierung durch VLANs
- IP-Whitelisting für administrative Zugänge und kritische Systeme (sofern technisch sinnvoll und möglich)
- Intrusion-Prevention durch automatische Sperrung bei Anmeldefehlversuchen (z.B. Fail2Ban, sofern technisch sinnvoll und möglich)

Gerätesicherheit:
- Verschlüsselung mobiler IT-Systeme (Laptops, Notebooks)
- Verschlüsselung mobiler Datenträger
- Verschlüsselung der Datensicherungssysteme
- Regelmäßige Sicherheitsupdates für Betriebssysteme und Anwendungen

Session-Management:
- Automatische Sitzungstrennung bei Inaktivität (sofern technisch sinnvoll und möglich)
- Automatische Abmeldung nach definierten Zeiträumen (sofern technisch sinnvoll und möglich)

2.5 Zugriffskontrolle

Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Berechtigungsmanagement:
- Berechtigungskonzept mit rollenbasierten Zugriffsrechten (RBAC)
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren ist auf das Notwendigste reduziert
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
- Unverzüglicher Entzug von Zugriffsrechten bei Ausscheiden von Mitarbeitern oder Änderung von Aufgabenbereichen

Zugriffssicherung:
- Passwortrichtlinie inkl. Mindestlänge und Komplexitätsanforderungen
- Nachvollziehbarkeit von Änderungen durch Versionierung und Logging (sofern technisch möglich)

Datenträgerverwaltung:
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern
- Physische Löschung oder kryptographische Vernichtung von Datenträgern vor Wiederverwendung oder Entsorgung
- Ordnungsgemäße Vernichtung von Datenträgern und Dokumenten (DIN 66399)
- Einsatz von Aktenvernichtern bzw. zertifizierten Dienstleistern für die Datenträgervernichtung
- Dokumentation der Vernichtung

Digitale Datenverarbeitung:
- Getrennte Verarbeitung nach Mandanten/Kunden (siehe Punkt 1: Zweckbindung)
- Zugriffsbeschränkungen auf Dateiebene durch ACLs
- Verschlüsselte Speicherung sensibler Daten

2.6 Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Protokollierung und Nachvollziehbarkeit:
- Protokollierung der Eingabe, Änderung und Löschung von Daten in kritischen Systemen (sofern technisch möglich)
- Verbindungsprotokolle im Rahmen der technischen Möglichkeiten der eingesetzten Tools (erfolgt nur nach gesonderter Beauftragung)
- Nachvollziehbarkeit durch individuelle Benutzernamen
- Versionierung und Änderungshistorie in Systemen (sofern verfügbar)

Berechtigungsvergabe:
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Dokumentation der Datenherkunft:
- Aufbewahrung von E-Mails, Tickets und digitalen Formularen
- Anrufhistorie zur Nachvollziehbarkeit von telefonischen Aufträgen

2.7 Auftragskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die von Unterauftragnehmern / Subunternehmern des Auftragnehmers verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und des Auftragnehmers verarbeitet werden können:

Auswahl und Beauftragung:

- Sorgfältige Auswahl von Subunternehmern unter Datenschutz- und Sicherheitsgesichtspunkten
- Abschluss schriftlicher Auftragsverarbeitungsverträge mit allen Subunternehmern

Verpflichtungen des Subunternehmers:

- Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Vereinbarung wirksamer Kontrollrechte (Audit-Rechte, Auskunftsrechte)

Aktuelle Subunternehmer:

- Änderungen werden dem Auftraggeber mitgeteilt

2.8 Transport- bzw. Weitergabekontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

Verschlüsselte Datenübertragung:

- Einsatz von VPN-Tunneln für Remote-Zugriffe und Standortverbindungen
- Verschlüsselung der Kommunikationswege (TLS/SSL für Webdienste, verschlüsselte E-Mail-Übertragung)
- HTTPS für alle webbasierten Anwendungen und Dienste
- Verschlüsselte Protokolle für administrative Zugriffe (SSH, SFTP)

Sichere Datenübermittlung:

- Nutzung verschlüsselter Filesharing-Lösungen oder verschlüsselter E-Mail-Anhänge bei sensiblen Daten
- Passwortschutz bei der Weitergabe sensibler Dokumente
- Separate Übermittlung von Passwörtern über andere Kommunikationskanäle

Physischer Transport:

- Verschlüsselung physischer Datenträger bei Transport
- Sichere und verdeckte Verwahrung von Datenträgern beim Transport
- Verzicht auf unverschlüsselte Datenträger für sensible Informationen

Protokollierung:

- Dokumentation von Datenübermittlungen bei größeren Datenmengen im Ticket System

3. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Rechenzentrumsinfrastruktur (Hetzner):

- Hosting kritischer Systeme in professionellen Rechenzentren mit:
  - Unterbrechungsfreier Stromversorgung (USV)

- Klimatisierung und Überwachung von Temperatur/Feuchtigkeit
- Brandschutz- und Löschanlagen
- Zutrittskontrollen und Alarmsystemen
- Redundanten Netzwerkanbindungen

- Nutzung zertifizierter Rechenzentren (ISO 27001, etc.)

Backup- und Wiederherstellungskonzept:

- Regelmäßige automatisierte Backups aller kritischen Systeme und Daten
- Aufbewahrung von Datensicherungen an geografisch getrennten Standorten
- Verschlüsselte Speicherung der Backups

Notfallvorsorge:

- Dokumentation des Sytems für Wiederherstellungsprozeduren
- Kontaktdaten und Eskalationswege für Notfälle

4. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Hier ist die vollständige Subunternehmer-Liste:

Hinweis: Die nachfolgende Liste umfasst sämtliche von der Berz Systems GmbH potenziell eingesetzten Unterauftragsverarbeiter. Ob diese im konkreten Auftragsverhältnis tatsächlich zum Einsatz kommen, hängt von den jeweils beauftragten Leistungen ab.

Dienstleister	Zweck & Daten	Land	Status
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting, Server, E-Mail-Dienste, Offsite-Backups	EU (Deutschland, Finnland)	aktiv
Heinlein Hosting GmbH Schwedter Straße 8/9A 10119 Berlin Deutschland	Mail Hosting, Kalender & Kontakte, Cloud Speicher, Video Call Anbieter	Deutschland	aktiv
easybell GmbH Brückenstraße 5a 10179 Berlin Deutschland	SIP-Trunk, Hotline, Telefonie-Dienste	Deutschland	aktiv
Bitwarden Inc. 1 North Calle Cesar Chavez, Suite 102 Santa Barbara, CA 93103 USA	Passwort-Tresor / Passwort-Management **Sicherheit:** Alle Daten sind End-to-End verschlüsselt (E2E) mit Zero-Knowledge-Architektur (extern auditiert). Bitwarden hat keinen Zugriff auf gespeicherte Passwörter oder Inhalte. **Drittlandtransfer:** Aufgrund der Zero-Knowledge-Architektur und der ausschließlich clientseitigen Ver- und Entschlüsselung liegen	EU (Cloud-Infrastruktur)	aktiv

	bei Bitwarden Inc. (und etwaigen US-Subprozessoren) zu keiner Zeit Klartextdaten oder die zur Entschlüsselung erforderlichen Schlüssel vor. Ein funktionaler Drittlandtransfer personenbezogener Daten i.S.d. Art. 44 ff. DSGVO findet daher nach derzeitiger Bewertung der Aufsichtspraxis nicht statt; ein etwaiger Zugriff nach US CLOUD Act bliebe ohne Erkenntniswert. Ergänzend gelten EU-Standardvertragsklauseln gem. Art. 46 DSGVO.		
Haufe Service Center GmbH Munzinger Straße 9 79111 Freiburg Deutschland	Rechnungserstellung, Buchhaltung (Lexware)	Deutschland	aktiv
Dynalist Inc. (Obsidian Sync) 115 George St, Suite 350 Oakville, ON, L6J 0A2 Kanada	Dokumentations- und Notiz-Synchronisierung **Verarbeitete Daten:** Kundendaten, Projektdokumentation **Sicherheit:** End-to-End-Verschlüsselung (AES-256) mit Zero-Knowledge-Architektur. Anbieter hat keinen Zugriff auf unverschlüsselte Inhalte. **Drittlandtransfer:** Aufgrund der Zero-Knowledge-Architektur und der ausschließlich clientseitigen Ver- und Entschlüsselung liegen beim Anbieter zu keiner Zeit Klartextdaten oder die zur Entschlüsselung erforderlichen Schlüssel vor. Ein funktionaler Drittlandtransfer personenbezogener Daten i.S.d. Art. 44 ff. DSGVO findet daher nach derzeitiger Bewertung der Aufsichtspraxis nicht statt. Für Kanada besteht ergänzend ein Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO) für kommerzielle Organisationen unter PIPEDA.	Frankfurt, EU (Cloud-Infrastruktur)	aktiv
Mistral AI 15 rue des Halles	KI-Assistent: Verarbeitung von Support-Tickets, Kundenanfragen, E-Mail-Kommunikation; Automatisierung von	EU (Frankreich), variable	aktiv

75001 Paris Frankreich	Dokumentation; KI-gestützte Analyse **Verarbeitete Daten:** Kontaktdaten, Kommunikationsinhalte, technische Nutzungsdaten **Besonderheit:** Opt-out vom KI-Training aktiviert; keine Verarbeitung besonderer Kategorien gem. Art. 9 DSGVO **Drittlandtransfer:** Über Subprozessoren möglich, abgesichert durch EU-Standardvertragsklauseln gem. Art. 46 DSGVO **Zertifizierungen:** ISO 27001, SOC 2, GDPR-DPA	Subprozessor-Standorte	
Microsoft Ireland Operations Limited 70 Sir John Rogerson's Quay Dublin 2, D02 R296 Irland Kontakt: eureg@microsoft.com	Azure OpenAI Service & Azure Cloud: KI-gestützte Verarbeitung von Support-Tickets, Kundenanfragen, E-Mails; Automatisierung von Dokumentation **Verarbeitete Daten:** Kontaktdaten, Kommunikationsinhalte, API-Aufrufe, Token-Nutzung **Besonderheit:** Keine Nutzung von Kundendaten für KI-Training; Modified Abuse Monitoring (Zero Data Retention); EU Data Boundary; Customer Lockbox aktiviert; keine Verarbeitung besonderer Kategorien gem. Art. 9 DSGVO **Drittlandtransfer:** Minimiert durch EU Data Boundary und regionale EU-Rechenzentren (Deutschland: Frankfurt, Berlin); bei Transfers abgesichert durch EU-US Data Privacy Framework gem. Art. 45 DSGVO sowie EU-Standardvertragsklauseln gem. Art. 46 DSGVO **Zertifizierungen:** ISO 27001/17/18/701, ISO 42001, SOC 1/2/3 Type 2, BSI C5:2020, HITRUST CSF v11	Datenverarbeitung in der EU Region (Irland, Deutschland, Schweden, Frankreich, Niederlande)	geplant
Twilio Inc. **Worldwide Headquarters:** 101 Spear Street,	SMS-Versand, RCS-Chats, Nachrichtenversand **Drittlandtransfer:** USA, abgesichert durch EU-	Global (USA, EU)	aktiv

5th Floor San Francisco, CA 94105 USA **EEA Headquarters:** Twilio Ireland Limited 70 Sir John Rogerson's Quay Dublin 2, D02 R296 Irland	US Data Privacy Framework und EU-Standardvertragsklauseln gem. Art. 46 DSGVO		
Sunny Valley Cyber Security Inc. (d.b.a. Zenarmor) 10080 N. Wolfe Rd., Suite SW3-200 Cupertino, CA 95014 USA EU-Büro: Frankfurt, Deutschland	SASE/NGFW-Lösung: Netzwerk-Sicherheit, Traffic-Filterung, Threat Intelligence, Web-Kategorisierung **Verarbeitete Daten:** IP-Adressen, Netzwerk-Metadaten, Geräte-Identifikatoren **Besonderheit:** Traffic-Verarbeitung primär lokal („Inspect Locally, Manage Centrally") **Drittlandtransfer:** USA, abgesichert durch EU-US Data Privacy Framework und EU-Standardvertragsklauseln gem. Art. 46 DSGVO **Zertifizierungen:** SOC 2 Type II, ISO/IEC 27001	Global (USA, EU, Kanada, Türkei)	aktiv
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg Deutsche Niederlassung: Anni-Albers-Str. 21, 80807 München Kontakt: aws-EU-privacy@amazon.com	KI-Plattform (AWS Bedrock, S3, EC2/Compute): Verarbeitung und Auswertung von Support-Tickets, Kundenanfragen, E-Mail-Kommunikation; Automatisierung von Dokumentationsprozessen; KI-gestützte Analyse und Texterstellung; KI-gestützte Auswertung von System-Logs, Konfigurationsdateien und Code-Snippets im Rahmen von Wartung, Fehleranalyse und DevOps; agentische Workflows mit kontrolliertem Tool-Zugriff (z.B. via Model Context Protocol / MCP) auf Drittsysteme im Rahmen der jeweils beauftragten Leistung **Verarbeitete Daten:** Kontaktdaten (Name, E-	Luxemburg (EU-Hauptsitz), Deutschland (Niederlassung) Datenverarbeitung in der EU Region (Frankfurt)	aktiv

	Mail, Telefon), Kommunikationsinhalte (Tickets, E-Mails, Anfragen, Prompt-Inputs), technische Nutzungsdaten (IP-Adressen, Zeitstempel, Session-IDs), System-Logs und Telemetrie, Konfigurationsdaten, Code-Fragmente **Besonderheit:** Keine Verwendung von Kundendaten für KI-Training; Prompts und Completions werden nicht gespeichert oder geloggt (Zero Data Retention); KI-Modellanbieter (einschließlich Anthropic für die Claude-Modellfamilie sowie weitere via Bedrock angebotene Foundation Models) haben keinen Zugriff auf Kundendaten – Inferenz erfolgt ausschließlich innerhalb der AWS-Infrastruktur in der EU-Region Frankfurt (eu-central-1); keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO **Zertifizierungen:** GDPR-konformes Data Processing Addendum, ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 1/2/3 Type II, BSI C5:2020 Type 2		
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland Deutsche Niederlassung: Google Germany GmbH, ABC-Straße 19, 20354 Hamburg Kontakt: https://cloud.google.com/contact	KI-Plattform (Vertex AI, Gemini API, Compute Engine, Cloud Storage): Verarbeitung und Auswertung von Support-Tickets, Kundenanfragen, E-Mail-Kommunikation; Automatisierung von Dokumentationsprozessen; KI-gestützte Analyse und Texterstellung; KI-gestützte Auswertung von System-Logs, Konfigurationsdateien und Code-Snippets im Rahmen von Wartung, Fehleranalyse und DevOps; agentische Workflows mit kontrolliertem Tool-Zugriff (z.B. via Model Context Protocol / MCP) auf Drittsysteme im Rahmen der jeweils beauftragten Leistung **Verarbeitete Daten:** Kontaktdaten (Name, E-Mail, Telefon), Kommunikationsinhalte, technische Nutzungsdaten (IP-Adressen, Zeitstempel, Session-IDs), System-Logs und Telemetrie, Konfigurationsdaten, Code-Fragmente	Irland (EU-Vertragspartner), Deutschland (Niederlassung) Datenverarbeitung in der EU Region (Frankfurt, Berlin)	aktiv

	Besonderheit: Keine Verwendung von Kundendaten für KI-Training bei Vertex AI Enterprise; Prompts/Completions Zero-Retention; KI-Modellanbieter (einschließlich Google sowie weitere via Vertex AI Model Garden bereitgestellte Foundation Models) haben keinen Zugriff auf Kundendaten – Inferenz erfolgt ausschließlich innerhalb der Google-Cloud-Infrastruktur in den EU-Regionen Frankfurt/Berlin; keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO **Zertifizierungen:** Cloud Data Processing Addendum (CDPA), ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 42001, SOC 1/2/3, BSI C5:2020 Type 2		
The Infrastructure Company GmbH Parkstrasse 42 47877 Willich Deutschland	Mail Hosting (Managed Mailcow): E-Mail-Server-Betrieb und -Verwaltung, E-Mail-Empfang und -Versand, Postfachverwaltung **Verarbeitete Daten:** E-Mail-Inhalte und -Metadaten (Absender, Empfänger, Betreff, Datum), Anhänge, Zugangsdaten (Benutzerkonten, Postfächer)	Deutschland	aktiv
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Irland Deutsche Niederlassung: Google Germany GmbH, ABC-Straße 19, 20354 Hamburg Kontakt: support.google.com/cloud/contact/dpo	Google Workspace (Gmail, Google Calendar, Google Drive, Google Meet): E-Mail-Dienste, Kalender, Dokumentenablage und Zusammenarbeit **Verarbeitete Daten:** Kommunikationsinhalte (E-Mails, Kalendereinträge), Dateiinhalte (Drive/Docs), Kontaktdaten, Nutzungsmetadaten **Besonderheit:** Cloud Data Processing Addendum (CDPA); Data Regions = EU konfiguriert (Datenresidenz EU); keine Verarbeitung besonderer Kategorien gem. Art. 9 DSGVO **Drittlandtransfer:** USA (Google LLC als Mutterkonzern, US CLOUD Act), abgesichert durch EU-Standardvertragsklauseln gem. Art. 46 DSGVO (SCC 2021/914 Modul 2 & 3);	Irland (EU-Vertragspartner) Datenverarbeitung in der EU (Data Regions = EU)	aktiv

	Transfer Impact Assessment (TIA) dokumentiert **Zertifizierungen:** ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 1/2/3		
OVH SAS 2 rue Kellermann 59100 Roubaix Frankreich Deutsche Tochter: OVH GmbH, Oskar-Jäger-Straße 173/K6, 50825 Köln Kontakt: dpo@ovh.com	Cloud Computing, Hosting, Server-Infrastruktur, KI-Workloads: Betrieb von Anwendungen, Datenverarbeitung, Backup-Infrastruktur **Verarbeitete Daten:** Kundendaten (je nach konfigurierter Workload), technische Metadaten, Backupdaten **Besonderheit:** Rein europäischer Anbieter (kein US CLOUD Act); EU-Rechenzentren wählbar (u. a. Limburg/DE, Frankreich, Polen); keine Verarbeitung außerhalb EU bei EU-Regionsauswahl **Zertifizierungen:** ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 1/2 Type II, HDS	EU (Frankreich, Deutschland u. a.)	aktiv
Scaleway S.A.S. 8 rue de la Ville l'Évêque 75008 Paris Frankreich Kontakt: privacy@scaleway.com, dpo@iliad.fr	Cloud Computing, KI-Inferenz (Generative APIs / Managed Inference), Server-Hosting: KI-gestützte Verarbeitung, Diktat-Pipelines, Dokumentenanalyse, Texterstellung **Verarbeitete Daten:** Prompt-Eingaben, Kommunikationsinhalte, technische Nutzungsdaten (IP-Adressen, Zeitstempel) **Besonderheit:** Rein europäischer Anbieter (Iliad-Gruppe, kein US CLOUD Act); KI-Dienste ausschließlich auf EU-Infrastruktur ohne Drittanbieter-Beteiligung; Default EU-Verarbeitung; keine Verarbeitung besonderer Kategorien gem. Art. 9 DSGVO **Zertifizierungen:** ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II, HDS	EU (Frankreich, Niederlande, Polen, Italien)	aktiv